МИНОБРНАУКИ РОССИИ
федеральное государственное бюджетное образовательное учреждение
высшего образования
«Самарский государственный технический университет»
(ФГБОУ ВО «СамГТУ»)

УТВЕРЖДАЮ:
Первый проректор-проректор по учебной работе
_____ / Д.Е. Овчинников
"_____" _____ 20___ г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Б1.В.ДВ.01.19 «Кибербезопасность интернета вещей»

Код и направление подготовки (специальность)	09.03.04 Программная инженерия
Направленность (профиль)	Программная инженерия
Квалификация	Бакалавр
Форма обучения	Заочная
Год начала подготовки	2023
Институт / факультет	Институт автоматики и информационных технологий
Выпускающая кафедра	кафедра «Информатика и вычислительная техника»
Кафедра-разработчик	кафедра "Информационно-измерительная техника"
Объем дисциплины, ч. / з.е.	108 / 3
Форма контроля (промежуточная аттестация)	Экзамен

Самара 2023

Б1.В.ДВ.01.19 «Кибербезопасность интернета вещей»

Рабочая программа дисциплины разработана в соответствии с требованиями ФГОС ВО по направлению подготовки (специальности) **09.03.04 Программная инженерия**, утвержденного приказом Министерства образования и науки РФ от № 920 от 19.09.2017 и соответствующего учебного плана.

Разработчик РПД:

Доцент, кандидат технических наук, доцент (должность, степень, ученое звание)	Е.В Мельников (ФИО)
Заведующий кафедрой	Е.Е. Ярославкина, кандидат технических наук, доцент (ФИО, степень, ученое звание)

СОГЛАСОВАНО:

Председатель методического совета факультета / института (или учебно-методической комиссии)	Я.Г Стельмах, кандидат педагогических наук, доцент (ФИО, степень, ученое звание)
Руководитель образовательной программы	С.П. Орлов, доктор технических наук, профессор (ФИО, степень, ученое звание)
Заведующий выпускающей кафедрой	А.В. Чуваков, кандидат химических наук, доцент (ФИО, степень, ученое звание)

Содержание

1. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы 4
2. Место дисциплины (модуля) в структуре образовательной программы 4
3. Объем дисциплины (модуля) в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся 5
4. Содержание дисциплины (модуля), структурированное по темам (разделам), с указанием отведенного на них количества академических часов и видов учебных занятий 6
4.1 Содержание лекционных занятий 6
4.2 Содержание лабораторных занятий 7
4.3 Содержание практических занятий 8
4.4. Содержание самостоятельной работы 8
5. Перечень учебной литературы и учебно-методического обеспечения по дисциплине (модулю) 9
6. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения 9
7. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», профессиональных баз данных, информационно-справочных систем 10
8. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине (модулю) 10
9. Методические материалы 10
10. Фонд оценочных средств по дисциплине (модулю) 12

1. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы

Наименование категории (группы) компетенций	Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Результаты обучения (знать, уметь, владеть, соотнесенные с индикаторами достижения компетенции)
Профессиональные компетенции			
Не предусмотрено	ПК-1 Способность использования различных технологий разработки программного обеспечения	ПК-1.1 Знает методы планирования проектных работ	Знать методы планирования проектных работ
		ПК-1.2 Умеет выбирать методы разработки требований к системе и шаблоны документов требований к ним	Уметь выбирать методы разработки требований к системе и шаблоны документов требований к ним
		ПК-1.3 Владеет способами разработки требований к системе	Владеть способами разработки требований к системе
	ПК-7 Способность выявления и исключение требований к системе и подсистеме, избыточно и необоснованно ограничивающих пространство концептуальных и технических решений	ПК-7.1 Знает атрибуты и методы проверки и обеспечения качества требований к системе и подсистеме	Знать атрибуты и методы проверки и обеспечения качества требований к системе и подсистеме
		ПК-7.2 Умеет выявлять и устранять неоднозначности в толковании требований к системе и подсистеме	Уметь выявлять и устранять неоднозначности в толковании требований к системе и подсистеме
		ПК-7.3 Владеет навыками определения источников информации для требований к системе	Владеть навыками определения источников информации для требований к системе

2. Место дисциплины (модуля) в структуре образовательной программы

Место дисциплины (модуля) в структуре образовательной программы: **вариативная часть**

Код компетенции	Предшествующие дисциплины	Параллельно осваиваемые дисциплины	Последующие дисциплины
ПК-1	Web-программирование; Алгоритмы и структуры данных; Дискретная математика (продвинутый); Разработка систем на базе ПЛИС; Язык программирования JavaScript; Язык программирования Python; Язык программирования C#; Язык программмрования Java	Методология автоматизации технологических процессов разработки ПО; Организация компьютерных систем	Выполнение и защита выпускной квалификационной работы; Методы параллельных вычислений; Мультиагентные системы; Программирование для суперкомпьютерных систем; Производственная практика: технологическая (проектно-технологическая) практика; Технологии виртуальной и дополненной реальности; Управление разработкой ПО
ПК-7	Инженерное моделирование в Blender		Выполнение и защита выпускной квалификационной работы; Конструирование ПО; Производственная практика: преддипломная практика; Производственная практика: эксплуатационная практика; Технологии обработки больших данных

3. Объем дисциплины (модуля) в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся

Вид учебной работы	Всего часов / часов в электронной форме	7 семестр часов / часов в электронной форме
Аудиторная контактная работа (всего), в том числе:	8	8
Лабораторные работы	4	4
Лекции	4	4
Самостоятельная работа (всего), в том числе:	91	91
подготовка к зачету	75	75
подготовка к лабораторным работам	16	16
Контроль	9	9
Итого: час	108	108
Итого: з.е.	3	3

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

учебных занятий

№ раздела	Наименование раздела дисциплины	Виды учебной нагрузки и их трудоемкость, часы				
		ЛЗ	ЛР	ПЗ	СРС	Всего часов
1	Кибербезопасность: основные понятия и определения.	2	0	0	15	17
2	Защита IOT систем	2	0	0	30	32
3	Особенности защиты OT систем по отраслям	0	4	0	46	50
	Контроль	0	0	0	0	9
	Итого	4	4	0	91	108

4.1 Содержание лекционных занятий

№ занятия	Наименование раздела	Тема лекции	**Содержание лекции** (перечень дидактических единиц: рассматриваемых подтем, вопросов)	Количество часов / часов в электронной форме
7 семестр				
1	Кибербезопасность: основные понятия и определения.	Цифровизация и цифровая трансформация экономики	Концепции, цели и задачи. Цифровизация внутренних процессов компании (предоставление услуг, операционная деятельность, управление бизнес-процессами). Корпоративные информационные системы. Цифровые технологии как инструмент решения задач цифровой трансформации. Цифровые бизнес-процессы и цифровая культура. Прогресс и проблемы безопасности. Национальная программа «Цифровая экономика Российской Федерации 2024». Проблемы информационной, компьютерной и кибербезопасности. Правовые основы информационной безопасности.	2

2	Защита IOT систем	Кибербезопасность в цифровых технологиях и цифровой трансформации	Интернет, мобильная связь, облака и облачные вычисления, дистанционное обучение, виртуальная и дополненная реальность, искусственный интеллект и машинное обучение, цифровой маркетинг, Интернет вещей. Цифровые трансформации и мировоззрение. Проблемы цифровизации, культуры, образования и безопасности. Человеческий фактор и проблемы кибербезопасности. Вирусы и программы-вымогатели. Основные правила компьютерной «гигиены»: пароли и их обновление, отношение к непонятным ссылкам, работа в социальных сетях. Цифровые технологии и трансформации в задачах управления финансами, персоналом, отношениями с поставщиками, транспортной деятельностью предприятия. Преимущества и выгоды, предоставляемые корпоративными информационными системами (КИС). Проблемы компьютерной и информационной безопасности в КИС. Требования к защите информации, не составляющей государственной тайны, содержащейся в государственных информационных системах (Требования ФСТЭК России). Защита передаваемых электронных данных. Электронная подпись. Классы безопасности электронных систем.	2
			Итого за семестр:	**4**
			Итого:	**4**

4.2 Содержание лабораторных занятий

№ занятия	**Наименование раздела**	**Тема лабораторного занятия**	**Содержание лабораторного занятия** (перечень дидактических единиц: рассматриваемых подтем, вопросов)	**Количество часов / часов в электронной форме**
7 семестр				
1	Особенности защиты ОТ систем по отраслям	Мониторинг влажности и температуры. Работа с устройством через проводное подключение	Контроль влажности и температуры. Работа через проводное подключение.	4
			Итого за семестр:	**4**
			Итого:	**4**

4.3 Содержание практических занятий

Учебные занятия не реализуются.

4.4. Содержание самостоятельной работы

Наименование раздела	**Вид самостоятельной работы**	**Содержание самостоятельной работы** (перечень дидактических единиц: рассматриваемых подтем, вопросов)	**Количество часов**
7 семестр			
Кибербезопасность: основные понятия и определения.	подготовка к зачету	Кибербезопасность (информационная безопасность) киберфизических систем, кибербезопасность в «Интер-нет-вещей»: основные стандарты, понятия, определения. Киберфизические системы и «Интернет-вещей»: обзор основных проблем, связанных с кибер-безопасностью; основные угрозы и уязвимости в сфере кибербезопасности.	15
Защита IOT систем	подготовка к зачету	Семиуровневая модель OSI. Протоколы интернета вещей. Классификация и описание возможных угроз, применительно к области IoT. Типовые примеры атак на компоненты систем IoT. Риски при использовании устройств IoT. Классификация. Отраслевые сетевые стандарты и модели для IoT под требования безопасности Канал связи. Проводные и беспроводные сетевые протоколы и их уязвимости. Виды уязвимостей. Методы защиты. Структуры систем. Развертывание. Уязвимость. Типовые методики. Межсетевые экраны. VPN. Шифрование.	30
Особенности защиты ОТ систем по отраслям	подготовка к зачету	Умные устройства. Сервис. Безопасность. Домашние животные. Технология. Безопасность. Качество. Мониторинг. Контроль трафика. Контроль водителя. Энеркоконтроль. Сбор данных. Балансовая граница. Измерение. Состав систем (категории систем, классификация), зрелость Smart City: понятие, критерии оценки, угрозы, риски и проблемы, модель угроз (структура, особенности), обзор стандартов по направлению «Умный город» (Smart City).	30
Особенности защиты ОТ систем по отраслям	подготовка к лабораторным работам	Мониторинг влажности и температуры. Работа с устройством через проводное подключение.	16
		Итого за семестр:	**91**

	Итого:	**91**

5. Перечень учебной литературы и учебно-методического обеспечения по дисциплине (модулю)

№ п/п	Библиографическое описание	Ресурс НТБ СамГТУ (ЭБС СамГТУ, IPRbooks и т.д.)
Основная литература		
1	Грингард, С. Интернет вещей : Будущее уже здесь : пер. с англ. / С. Грингард.- М., Точка, 2017Альпина Паблишер.- 198 с.	Книжный фонд
2	Кирсанов, Э.А. Обработка информации в пространственно-распределенных системах радиомониторинга.: статический и нейросетевой подходы / Э. А. Кирсанов, А. А. Сирота.- М., Физматлит, 2012.- 343 с.	Книжный фонд
Дополнительная литература		
3	Орлов, С.А. Программная инженерия : Технология разработки программного обеспечения : учеб. / С. А. Орлов .- 5е изд., обновл. и доп..- М., Питер , 2016.- 640 с.	Книжный фонд
4	Семененко, В.А. Информатика и вычислительная техника : Учеб.пособие / В.А.Семененко,Э.К.Скуратович .- 2-е изд.,стер..- М., Моск.гос.индустр.ун-т, 2006.- 271 с.	Книжный фонд

Доступ обучающихся к ЭР НТБ СамГТУ (elib.samgtu.ru) осуществляется посредством электронной информационной образовательной среды университета и сайта НТБ СамГТУ по логину и паролю.

6. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения

При проведении лекционных занятий используется мультимедийное оборудование.

Организовано взаимодействие обучающегося и преподавателя с использованием электронной ин-формационной образовательной среды университета.

№ п/п	Наименование	Производитель	Способ распространения
1	AdobeReader	AdobeSystemsIncorporated (Зарубежный)	Свободно распространяемое
2	Quartus 2 web edition V15.0	Intel (Зарубежный)	Свободно распространяемое
3	Архиватор 7-Zip	IgorPavlov (Зарубежный)	Свободно распространяемое
4	Операционная система MicrosoftWindows	Microsoft (Зарубежный)	Лицензионное
5	Пакет офисных программ LibreOffice	TheDocumentFoundation (Зарубежный)	Свободно распространяемое
6	Яндекс.Браузер	Яндекс (Отечественный)	Свободно распространяемое

7. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», профессиональных баз данных, информационно-справочных систем

№ п/п	Наименование	Краткое описание	Режим доступа
1	eLIBRARY.ru	http://www.eLIBRARY.ru/	Российские базы данных ограниченного доступа
2	Электронно-библиотечная система IPRbooks	http://www.iprbookshop.ru/	Российские базы данных ограниченного доступа
3	Электронная библиотека изданий СамГТУ	http://irbis.samgtu.local/cgi-bin/irbis64r_01/cgiirbis_64.exe	Российские базы данных ограниченного доступа

8. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине (модулю)

Лекционные занятия

Аудитории для лекционных занятий укомплектованы мебелью и техническими средствами обучения, служащими для представления учебной информации большой аудитории (наборы демонстрационного оборудования (проектор,экран, компьютер/ноутбук).

Лабораторные занятия

Для лабораторных занятий используется специализированная аудитория N410, 8 корпус, оснащенная компьютерами с ПО и лабораторными макетами с ПЛИС.

Самостоятельная работа

помещения длясамостоятельной работы оснащены компьютернойтехникой с возможностью подключения к сети «Интернет» и доступом к электроннойинформационно-образовательной среде СамГТУ:

- читальный зал НТБ СамГТУ (ауд. 200 корпус № 8; ауд. 125 корпус № 1;ауд. 41 Главный корпус библиотеки, ауд.0209 АСА СамГТУ);

- компьютерные классы(ауд. 310, 210 корпус № 8).

9. Методические материалы

Методические рекомендации при работе на лекции

До лекции студент должен просмотреть учебно-методическую и научную литературу по теме лекции с тем, чтобы иметь представление о проблемах, которые будут разбираться в лекции.

Перед началом лекции обучающимся сообщается тема лекции, план, вопросы, подлежащие рассмотрению, доводятся основные литературные источники. Весь учебный материал, сообщаемый преподавателем, должен не просто прослушиваться. Он должен быть активно воспринят, т.е. услышан, осмыслен, понят, зафиксирован на бумаге и закреплен в памяти. Приступая к слушанию нового учебного материала, полезно мысленно установить его связь с ранее изученным. Следя за техникой чтения лекции (акцент на существенном, повышение тона, изменение ритма, пауза и т.п.), необходимо вслед за преподавателем уметь выделять основные категории, законы и определять их содержание, проблемы, предполагать их возможные решения, доказательства и выводы. Осуществляя такую работу, можно значительно облегчить себе понимание учебного материала, его конспектирование и дальнейшее изучение.

Конспектирование лекции позволяет обработать, систематизировать и лучше сохранить полученную информацию с тем, чтобы в будущем можно было восстановить в памяти основные, содержательные моменты. Типичная ошибка, совершаемая обучающимся, дословное конспектирование речи преподавателя. Как правило, при записи «слово в слово» не остается времени на обдумывание, анализ и синтез информации. Отбирая нужную информацию, главные мысли, проблемы, решения и выводы, необходимо сокращать текст, строить его таким образом, чтобы потом можно было легко в нем разобраться. Желательно оставить в рабочих конспектах поля, на которых можно будет делать пометки из рекомендованной литературы, дополняющие материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений. С окончанием лекции работа над конспектом не может считаться завершенной. Нужно еще восстановить отдельные места, проверить, все ли понятно, уточнить что-то на консультации и т.п. с тем, чтобы конспект мог быть использован в процессе подготовки к практическим занятиям, зачету, экзамену. Конспект лекции – незаменимый учебный документ, необходимый для самостоятельной работы.

Методические рекомендации при работе на лабораторном занятии

Проведение лабораторной работы делится на две условные части: теоретическую и практическую.

Необходимыми структурными элементами занятия являются проведение лабораторной работы, проверка усвоенного материала, включающая обсуждение теоретических основ выполняемой работы.

Перед лабораторной работой, как правило, проводится технико-теоретический инструктаж по использованию необходимого оборудования. Преподаватель корректирует деятельность обучающегося в процессе выполнения работы (при необходимости). После завершения лабораторной работы подводятся итоги, обсуждаются результаты деятельности.

Возможны следующие формы организации лабораторных работ: фронтальная, групповая и индивидуальная. При фронтальной форме выполняется одна и та же работа (при этом возможны различные варианты заданий). При групповой форме работа выполняется группой (командой). При индивидуальной форме обучающимися выполняются индивидуальные работы.

По каждой лабораторной работе имеются методические указания по их выполнению, включающие необходимый теоретический и практический материал, содержащие элементы и последовательную инструкцию по проведению выбранной работы, индивидуальные варианты заданий, требования и форму отчётности по данной работе.

Методические рекомендации по выполнению самостоятельной работы

Организация самостоятельной работы обучающихся ориентируется на активные методы овладения знаниями, развитие творческих способностей, переход от поточного к индивидуализированному обучению с учетом потребностей и возможностей обучающегося.

Самостоятельная работа с учебниками, учебными пособиями, научной, справочной литературой, материалами периодических изданий и Интернета является наиболее эффективным методом получения дополнительных знаний, позволяет значительно активизировать процесс овладения информацией, способствует более глубокому усвоению изучаемого материала. Все новые понятия по изучаемой теме необходимо выучить наизусть и внести в глоссарий, который целесообразно вести с самого начала

изучения курса.

Самостоятельная работа реализуется:

- непосредственно в процессе аудиторных занятий;
- на лекциях, практических занятиях;
- в контакте с преподавателем вне рамок расписания;
- на консультациях по учебным вопросам, в ходе творческих контактов, при ликвидации задолженностей, при выполнении индивидуальных заданий и т.д.;
- в библиотеке, дома, на кафедре при выполнении обучающимся учебных и практических задач.

Эффективным средством осуществления обучающимся самостоятельной работы является электронная информационно-образовательная среда университета, которая обеспечивает доступ к учебным планам, рабочим программам дисциплин (модулей), практик, к изданиям электронных библиотечных систем.

10. Фонд оценочных средств по дисциплине (модулю)

Фонд оценочных средств представлен в приложении № 1.

Приложение 1 к рабочей программе дисциплины
Б1.В.ДВ.01.19 «Кибербезопасность интернета вещей»

Фонд оценочных средств
по дисциплине
Б1.В.ДВ.01.19 «Кибербезопасность интернета вещей»

Код и направление подготовки (специальность)	09.03.04 Программная инженерия
Направленность (профиль)	Программная инженерия
Квалификация	Бакалавр
Форма обучения	Заочная
Год начала подготовки	2023
Институт / факультет	Институт автоматики и информационных технологий
Выпускающая кафедра	кафедра «Информатика и вычислительная техника»
Кафедра-разработчик	кафедра "Информационно-измерительная техника"
Объем дисциплины, ч. / з.е.	108 / 3
Форма контроля (промежуточная аттестация)	Экзамен

Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы

Наименование категории (группы) компетенций	Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Результаты обучения (знать, уметь, владеть, соотнесенные с индикаторами достижения компетенции)
Профессиональные компетенции			
Не предусмотрено	ПК-1 Способность использования различных технологий разработки программного обеспечения	ПК-1.1 Знает методы планирования проектных работ	Знать методы планирования проектных работ
		ПК-1.2 Умеет выбирать методы разработки требований к системе и шаблоны документов требований к ним	Уметь выбирать методы разработки требований к системе и шаблоны документов требований к ним
		ПК-1.3 Владеет способами разработки требований к системе	Владеть способами разработки требований к системе
	ПК-7 Способность выявления и исключение требований к системе и подсистеме, избыточно и необоснованно ограничивающих пространство концептуальных и технических решений	ПК-7.1 Знает атрибуты и методы проверки и обеспечения качества требований к системе и подсистеме	Знать атрибуты и методы проверки и обеспечения качества требований к системе и подсистеме
		ПК-7.2 Умеет выявлять и устранять неоднозначности в толковании требований к системе и подсистеме	Уметь выявлять и устранять неоднозначности в толковании требований к системе и подсистеме
		ПК-7.3 Владеет навыками определения источников информации для требований к системе	Владеть навыками определения источников информации для требований к системе

Матрица соответствия оценочных средств запланированным результатам обучения

Код индикатора достижения компетенции	Результаты обучения	Оценочные средства	Текущий контроль успеваемости	Промежуточная аттестация
Кибербезопасность: основные понятия и определения.				
ПК-1.1 Знает методы планирования проектных работ	**Знать** методы планирования проектных работ	Вопросы к экзамену	Нет	Да
		Тестирование	Да	Нет
ПК-1.2 Умеет выбирать методы разработки требований к системе и шаблоны документов требований к ним	**Уметь** выбирать методы разработки требований к системе и шаблоны документов требований к ним	Тестирование	Да	Нет
ПК-1.3 Владеет способами разработки требований к системе	**Владеть** способами разработки требований к системе	Тестирование	Да	Нет
		Вопросы к экзамену	Нет	Да
ПК-7.1 Знает атрибуты и методы проверки и обеспечения качества требований к системе и подсистеме	**Знать** атрибуты и методы проверки и обеспечения качества требований к системе и подсистеме	Вопросы к экзамену	Нет	Да
		Тестирование	Да	Нет
ПК-7.2 Умеет выявлять и устранять неоднозначности в толковании требований к системе и подсистеме	**Уметь** выявлять и устранять неоднозначности в толковании требований к системе и подсистеме	Тестирование	Да	Нет
ПК-7.3 Владеет навыками определения источников информации для требований к системе	**Владеть** навыками определения источников информации для требований к системе	Вопросы к экзамену	Нет	Да
Защита IOT систем				
ПК-1.1 Знает методы планирования проектных работ	**Знать** методы планирования проектных работ	Вопросы к экзамену	Нет	Да
		Тестирование	Да	Нет
ПК-1.2 Умеет выбирать методы разработки требований к системе и шаблоны документов требований к ним	**Уметь** выбирать методы разработки требований к системе и шаблоны документов требований к ним	Тестирование	Да	Нет

ПК-1.3 Владеет способами разработки требований к системе	**Владеть** способами разработки требований к системе	Тестирование	Да	Нет
		Вопросы к экзамену	Нет	Да
ПК-7.1 Знает атрибуты и методы проверки и обеспечения качества требований к системе и подсистеме	**Знать** атрибуты и методы проверки и обеспечения качества требований к системе и подсистеме	Вопросы к экзамену	Нет	Да
		Тестирование	Да	Нет
ПК-7.2 Умеет выявлять и устранять неоднозначности в толковании требований к системе и подсистеме	**Уметь** выявлять и устранять неоднозначности в толковании требований к системе и подсистеме	Тестирование	Да	Нет
ПК-7.3 Владеет навыками определения источников информации для требований к системе	**Владеть** навыками определения источников информации для требований к системе	Тестирование	Да	Нет
		Вопросы к экзамену	Нет	Да
Особенности защиты ОТ систем по отраслям				
ПК-1.1 Знает методы планирования проектных работ	**Знать** методы планирования проектных работ	Вопросы к экзамену	Нет	Да
		Тестирование	Да	Нет
ПК-1.2 Умеет выбирать методы разработки требований к системе и шаблоны документов требований к ним	**Уметь** выбирать методы разработки требований к системе и шаблоны документов требований к ним	отчет по лабораторным работам	Да	Нет
ПК-1.3 Владеет способами разработки требований к системе	**Владеть** способами разработки требований к системе	отчет по лабораторным работам	Да	Нет
ПК-7.1 Знает атрибуты и методы проверки и обеспечения качества требований к системе и подсистеме	**Знать** атрибуты и методы проверки и обеспечения качества требований к системе и подсистеме	Тестирование	Да	Нет
		Вопросы к экзамену	Нет	Да

ПК-7.2 Умеет выявлять и устранять неоднозначности в толковании требований к системе и подсистеме	**Уметь** выявлять и устранять неоднозначности в толковании требований к системе и подсистеме	отчет по лабораторным работам	Да	Нет
ПК-7.3 Владеет навыками определения источников информации для требований к системе	**Владеть** навыками определения источников информации для требований к системе	отчет по лабораторным работам	Да	Нет

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

Формы текущего контроля успеваемости

Примерные тесты

1. Предположим, что вас попросили сделать систему - пожарную сигнализацию для фестиваля авторской песни в лесу. Энергопотребление системы не имеет значения, так как фестиваль длится всего неделю, и в следующем году состоится в другом месте. От вас попросили сделать систему максимально дешёвой. Датчик на базе какой микросхемы вы выберете?
   - SHT21
   - LMT01
   - LM75
   - BME280
2. Предположим, что вам поставили задачу сделать систему - автоматический инкубатор для цыплят. Погрешность измерения температуры в такой системе не должна превышать 0,3 градуса по Цельсию. Датчик на базе какой микросхемы вы выберете?
   - LMT01
   - BME280
   - LM75
   - SHT21
3. Какая из данных технологий способна образовывать самоорганизующуюся ячеистую сеть (mesh-сеть) по умолчанию, без дополнительных усилий?
   - WiFi
   - ZigBee
   - Bluetooth

   1248768
   - LoRa
4. Название JSON (JavaScript Object Notation) означает, что этот формат…
   - Был придуман, чтобы добавить к языку Java возможности скриптового программирования
   - Был уже в дальнейшем адаптирован для нужд языка JavaScript, а изначально назывался иначе
   - Может использоваться только в языке JavaScript
   - Исторически появился в языке JavaScript для передачи данных в Интернете
5. Если считать посимвольно, то наименьший объём при прочих равных всегда будет иметь сообщение в формате…
   - HTML
   - YAML
   - JSON
   - XML
6. Допустим, что вы конструируете устройство, которое должно знать о том, открыта ли дверь. Какой механизм протокола MQTT стоит использовать, чтобы новые подписчики сразу узнавали статус двери?
   - Retain
   - Network Pipe

- Last Will

- QoS

7. Механизм MQTT, называемый “Завещание” (“Last Will”), используется, чтобы:

   - Уведомить подписчиков о том, что есть проблема на стороне издателя

   - Оставить сообщение “до востребования”, то есть сделать его доступным для новых подписчиков

   - Гарантировать доставку сообщения

   - Уведомить издателя о проблеме с сетью

8. Что такое GPIO?

   - Регистры флагов текущего состояния процессора

   - Регистры ввода-вывода общего назначения

   - Индексные регистры

   - Регистры энергонезависимой памяти устройства

9. Реле, по сравнению с транзистором, имеет следующее преимущество:

   - Скорость срабатывания

   - Полная электрическая изоляция от выходной мощной цепи

   - Компактность

   - Меньший износ

10. Перед вами простой код примера для Paho в MQTT:

    ```
    import paho.mqtt.client as mqtt

    def on_connect(client, userdata, flags, rc):

    client.subscribe("$SYS/#")

    def on_message(client, userdata, msg):

    print(msg.topic+" "+str(msg.payload))

    client = mqtt.Client()

    client.on_connect = on_connect

    client.on_message = on_message

    client.connect("iot.eclipse.org", 1883, 60)

    client.loop_forever()
    ```

    В конце программы вы видите бесконечный цикл ожидания. Можно ли от него избавиться?

    - Цикл нельзя разрывать, иначе программа перестанет ожидать сообщения от сервера, и её работоспособность будет нарушена.

    - Да, цикл можно разорвать при помощи функций loop_start() и loop_stop()

11. Преимущества использования mock-объектов в том, что они…

    - Позволяют избавиться от ошибок компиляции, связанными с подключением несуществующих библиотек.

    - Защищают входы и выходы устройства от подачи избыточного напряжения, и как следствие, выгорания.

    - Ускоряют тестирование и отладку системы в случае, если замещаемый ими объект слишком медленный

    - Позволяют тестировать логику работы системы в отсутствие физических объектов

12. В одной из систем мониторинга влажности и температуры на фармацевтическом складе датчики в холодильнике опускаются в баночки, заполненные гликолем. Для чего?

    - Чтобы защитить датчики от механического повреждения

    - Чтобы защитить датчики от переохлаждения

    - Чтобы повысить чувствительность датчиков

    - Чтобы сгладить показания датчика в случае открытия дверцы

13. Для решения какой задачи вы точно не будете использовать технологию LoRa?

    - Измерение температуры тела коровы

    - Снятие показаний электронных счетчиков ЖКХ

    - Отслеживание местоположения транспорта в реальном времени

    - Экологический мониторинг реки на предмет слива промышленных отходов

14. Как достигается уникальность идентификатора устройства (DevEUI) в сетях LoRa?

    - Производитель конечных устройств назначает идентификатор из диапазона разрешённыхадресов

    - Никак не достигается, идентификатор можно свободно менять

    - Производитель приёмопередатчиков LoRa, компания Semtech, присваивает идентификаторкаждому чипу

15. Почему не стоит делать период опроса датчиков меньше 1 минуты, если мы работаем с системой LoRa?

    - Отправка и пересылка сообщений занимает слишком много времени, поэтому это создаст“затор” в сети

    - Период менее 1 минуты не поддерживается RIOT OS

    - Архитектура микроконтроллера не позволяет назначить период дробным числом

    - Датчик не успевает оцифровать показания

16. К какому из уровней модели OSI относится такой аспект, как форма разъёмов сетевых кабелей?

    - Физический

    - Передачи данных

    - Сетевой

    - Транспортный

    - Прикладной

17. Каждый из уровней в эталонных моделях OSI или TCP/IP...

    - Передаёт данные напрямую на соответствующий уровень системы-адресата

    - Общается со всеми уровнями

    - Общается только с нижестоящим и вышестоящим уровнем

18. LISTEN, CONNECT, ACCEPT, RECEIVE, SEND, DISCONNECT - это…

    - Протоколы

    - Сетевые службы

    - Уровни модели

    - Примитивы служб

    - Интерфейсы

19. Протокол MQTT-SN (Sensor Networks) на транспортном уровне предполагает использованиепротокола...

    - UDP

    - UDP-Lite

    - SCTP

    - TCP

20. В каком радиодиапазоне работает WiFi?

    - 915 МГц

    - 108 МГц

    - 868 МГц

    - 2450 МГц

    - 433 МГц

Формы промежуточной аттестации

Примерный перечень вопросов для подготовки к экзамену

1. Обработка данных в IoT.
2. Применение облачных технологий и сервисно-орентированных архитектур в IoT.
3. Уязвимости уровня прикладных программ.
4. Типовые примеры атак на компоненты систем IoT.
5. Классификация и описание возможных угроз, применительно к области IoT.
6. Риски при использовании устройств IoT.
7. Отраслевые сетевые стандарты и модели для IoT под требования безопасности.
8. Канал связи. Проводные и беспроводные сетевые протоколы и их уязвимости.
9. Методика оценки уязвимости и рисков в системе, содержащей устройства IoT.
10. Современные технологии в области безопасности IoT.
11. Основные понятия в области кибербезопасности Интернета вещей; основные угрозы, риски и уязвимости в сфере кибербезопасности Интернета вещей и критической информационной инфраструктуры;
12. Основные протоколы передачи данных и аутентификации, используемые в «Интернет вещей»;
13. Основные понятия в сфере функциональной безопасности;
14. Положения основных нормативных актов, регулирующих сферу безопасности критической информационной инфраструктуры Российской Федерации;
15. Архитектура основных подсистем обеспечения ИБ объектов КИИ;
16. Основные определения СМИБ и особенности построения СМИБ для объектов КИИ на промышленных объектах;
17. Положения нормативных актов, устанавливающих ответственность за нарушение требований законодательства РФ в сфере обеспечения безопасности КИИ и КВО ТЭК.
18. Основные средства обеспечения кибербезопасности (архитектура, принципы построения);
19. Принципы проектирования систем безопасности значимых объектов КИИ;
20. Состав и способы организации деятельности сил обеспечения кибербезопасности объектов КИИ;
21. Основные требования к специалистам в области кибербезопасности «Интернет-вещей»,критической информационной инфраструктуры;
22. Цели обеспечения кибербезопасности в «Интернет-вещей» для граждан;
23. Классификация и примеры продуктов «Интернет-вещей» для граждан, примеры угроз, уязвимостей, рисков;
24. Основные риски и проблемы кибербезопасности «Интернет-вещей» в сфере здравоохранения;
25. Основные риски и проблемы кибербезопасности для «Умного дома»;
26. Состав и классификация систем для «Умного города», критерии оценки безопасности, основных угроз, рисков и проблем, структуры и особенностей построения модели угроз;
27. Основные риски и проблемы кибербезопасности в Smart Grid;
28. Основные риски и проблемы кибербезопасности в Индустриальном Интернете вещей;
29. Примеры юридических инцидентов в области регулирования кибербезопасности «Интернета - вещей»;

Тесты по компетенциям

Направление подготовки: 09.03.04 Программная инженерия

Профиль: Программная инженерия

Дисциплина: Б1.В.ДВ.01.19 Кибербезопасность интернета вещей

№	Содержание задания	Ключ к ответу	Наименование темы РПД	Семестр
ПК-1: Способность использования различных технологий разработки программного обеспечения				
1	Прочитайте текст задания и выберите правильный ответ. Как называется интеграция вычислительных ресурсов в физические процессы, являющаяся основой IV промышленной революции? А) Облачные вычисления Б) Киберфизические системы (CPS) В) Социальные сети Г) Клиент-серверная архитектура	Б	Кибербезопасность: основные понятия и определения / Кибербезопасность киберфизических систем	7.0
2	Прочитайте текст задания и дайте развернутый ответ. В чем отличие киберфизической системы от обычной ИТ-системы?	Киберфизическая система напрямую взаимодействует с материальным миром через датчики и исполнительные механизмы, поэтому кибератака на неё может привести к физическим разрушениям.	Кибербезопасность: основные понятия и определения / Кибербезопасность киберфизических систем	nan
3	Прочитайте текст задания и дополните его. Для обеспечения кибербезопасности в «Умном городе» применяются международные и национальные _____ (например, ISO/IEC).	стандарты	Особенности защиты ОТ систем по отраслям / Умный город	nan
4	Прочитайте текст задания и дополните его. Основным стандартом описания сетевого взаимодействия является семиуровневая модель _____.	OSI	Защита IOT систем / Сетевые технологии и протоколы	nan
5	Прочитайте текст задания и установите последовательность. Приоритеты защиты (триада CIA) в промышленных IoT системах (традиционно): 1) Доступность (Availability) 2) Целостность (Integrity) 3) Конфиденциальность (Confidentiality)	1-2-3	Кибербезопасность: основные понятия и определения / Кибербезопасность киберфизических систем	nan
6	Прочитайте текст задания и установите последовательность. Порядок прохождения данных снизу вверх (по модели OSI): 1) Физический уровень 2) Сетевой уровень 3) Прикладной уровень	1-2-3	Защита IOT систем / Сетевые технологии и протоколы	7.0
7	Прочитайте текст задания и установите последовательность. Этапы типовой атаки на IoT-устройство: 1) Поиск открытых портов/сервисов 2) Эксплуатация известной уязвимости	1-2-3	Защита IOT систем / Атака на устройства IoT	7.0

	3) Закрепление в системе и кража данных			
8	Прочитайте текст задания и дайте развернутый ответ. Опишите основные угрозы безопасности в «Умном городе».	Нарушение работы светофоров, взлом систем водоснабжения и электропитания, слежка за гражданами через камеры, подмена данных в системах оповещения о ЧС.	Особенности защиты ОТ систем по отраслям / Умный город	nan
9	Прочитайте текст задания и установите соответствие. Сопоставьте уровень архитектуры IoT и решаемую задачу: А) Уровень восприятия Б) Сетевой уровень В) Прикладной уровень --- 1) Передача данных 2) Сбор данных датчиками 3) Обработка данных в облаке	А-2, Б-1, В-3	Защита IOT систем / Архитектура IoT систем	7.0
10	Прочитайте текст задания и выберите несколько правильных ответов. Какие параметры контролируются в транспортных IoT-системах? А) Состояние водителя Б) Трафик и заторы В) Уровень влажности в лесу Г) Местоположение груза	А, Б, Г	Особенности защиты ОТ систем по отраслям / Применение IoT в транспорте	7.0
11	Прочитайте текст задания и установите соответствие. Сопоставьте термин и определение: А) Уязвимость Б) Риск В) Межсетевой экран --- 1) Недостаток в защите 2) Устройство фильтрации трафика 3) Вероятный ущерб	А-1, Б-3, В-2	Защита IOT систем / Методика оценки уязвимости и рисков	7.0
12	Прочитайте текст задания и выберите правильный ответ. Какой протокол прикладного уровня чаще всего используется в IoT благодаря модели «издатель-подписчик»? А) HTTP Б) FTP В) MQTT Г) Telnet	В	Защита IOT систем / Сетевые технологии и протоколы	7.0

13	Прочитайте текст задания и выберите несколько правильных ответов. Что относится к компонентам «Умного дома» с точки зрения безопасности? А) Умные замки и камеры Б) Облачные сервисы управления В) Домашние животные без датчиков Г) Контроллеры освещения	А, Б, Г	Особенности защиты ОТ систем по отраслям / Известные применения IoT: Умный дом	7.0
14	Прочитайте текст задания и выберите несколько правильных ответов. Выберите характерные уязвимости беспроводных каналов связи в IoT системах: А) Перехват трафика (Sniffing) Б) Подмена данных (Spoofing) В) Физический обрыв оптоволокна Г) Создание помех (Jamming)	А, Б, Г	Защита IOT систем / Атака на устройства IoT	7.0
15	Прочитайте текст задания и выберите правильный ответ. Как классифицируются атаки, направленные на исчерпание ресурсов устройства IoT (батареи или памяти)? А) Фишинг Б) Атака на доступность (DoS) В) SQL-инъекция Г) Социальная инженерия	Б	Защита IOT систем / Угрозы IOT	7.0
ПК-7: Способность выявления и исключение требований к системе и подсистеме, избыточно и необоснованно ограничивающих пространство концептуальных и технических решений				
16	Прочитайте текст задания и дайте развернутый ответ. Почему сегментация сети важна для защиты IoT систем?	Она позволяет изолировать потенциально уязвимые устройства IoT от критически важных серверов и данных организации, предотвращая распространение атаки по всей сети.	Защита IOT систем / Новые технологии в области безопасности IoT	nan
17	Прочитайте текст задания и выберите правильный ответ. На каком уровне модели OSI работают сетевые шлюзы IoT, обеспечивая маршрутизацию пакетов? А) Физический Б) Канальный В) Сетевой Г) Сеансовый	В	Защита IOT систем / Сетевые технологии и протоколы	7.0
18	Прочитайте текст задания и дополните его. В системе «Умный дом» управление через интернет чаще всего реализуется с использованием _____ приложений.	облачных	Защита IOT систем / Локальные и облачные приложения	nan
19	Прочитайте текст задания и дополните его. Использование стандартных (заводских) _____ является самой частой причиной попадания IoT-устройств в ботнеты.	паролей	Защита IOT систем / Угрозы IOT	nan

20	Прочитайте текст задания и выберите правильный ответ. Какой риск является наиболее критичным при использовании медицинских IoT-устройств? А) Утеря пароля от почты Б) Угроза жизни и здоровью пациента В) Снижение скорости интернета Г) Неправильное отображение времени	Б	Защита IOT систем / Устройства IoT	7.0
21	Прочитайте текст задания и дополните его. Устройства, имеющие датчики и подключение к сети, но обладающие ограниченными вычислительными ресурсами, называют _____ устройствами.	IoT (или умными)	Защита IOT систем / Устройства IoT	nan
22	Прочитайте текст задания и установите соответствие. Сопоставьте тип атаки и её цель: А) MITM (Человек посередине) Б) Ransomware В) Brute-force --- 1) Подбор пароля 2) Перехват и изменение данных 3) Вымогательство выкупа	А-2, Б-3, В-1	Защита IOT систем / Угрозы IOT	7.0
23	Прочитайте текст задания и установите последовательность. Жизненный цикл IoT-устройства с точки зрения защиты: 1) Безопасная настройка и установка 2) Мониторинг и регулярное обновление 3) Безопасная утилизация (очистка данных)	1-2-3	Защита IOT систем / Устройства IoT	7.0
24	Прочитайте текст задания и выберите правильный ответ. Как называется технология защиты, создающая зашифрованный канал связи для IoT-устройств в открытой сети? А) HTTP Б) VPN В) VLAN Г) DNS	Б	Защита IOT систем / Новые технологии в области безопасности IoT	7.0
25	Прочитайте текст задания и установите последовательность. Порядок оценки рисков в системе IoT: 1) Определение ценности активов 2) Идентификация актуальных угроз 3) Расчет уровня риска	1-2-3	Защита IOT систем / Методика оценки уязвимости и рисков	7.0

26	Прочитайте текст задания и установите соответствие. Сопоставьте технологию и её назначение: А) Шифрование Б) VPN В) Локальное приложение --- 1) Безопасный туннель 2) Конфиденциальность данных 3) Автономная работа в периметре объекта	А-2, Б-1, В-3	Защита IOT систем / Локальные и облачные приложения	7.0
27	Прочитайте текст задания и выберите несколько правильных ответов. Какие задачи решаются при внедрении IoT в энергетике? А) Энергоконтроль Б) Сбор данных на балансовой границе В) Автоматизация полива газонов Г) Дистанционное измерение параметров сети	А, Б, Г	Особенности защиты ОТ систем по отраслям / Применение IoT в энергетике	7.0
28	Прочитайте текст задания и установите соответствие. Сопоставьте отрасль и фокус безопасности: А) Промышленность (IIoT) Б) Умный город В) Транспорт --- 1) Стандарты Smart City 2) Качество продукции и безопасность технологии 3) Беспилотное управление	А-2, Б-1, В-3	Особенности защиты ОТ систем по отраслям / Умный город, Промышленность	7.0
29	Прочитайте текст задания и выберите несколько правильных ответов. Какие уязвимости характерны для прикладного уровня (ПО) IoT-систем? А) Небезопасные API Б) Отсутствие авторизации В) Межсайтовый скриптинг (XSS) Г) Плохая освещенность датчиков	А, Б, В	Защита IOT систем / Уязвимости уровня прикладных программ	7.0
30	Прочитайте текст задания и дайте развернутый ответ. Какую роль играет «безопасная загрузка» (Secure Boot) в устройствах IoT?	Она гарантирует, что на устройстве запускается только доверенное программное обеспечение от производителя, предотвращая замену прошивки на вредоносную.	Защита IOT систем / Устройства IoT	nan

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

Характеристика процедуры текущей и промежуточной аттестации по дисциплине

Таблица 1

№ п/п	Наименование оценочного средства	Периодичность и способ проведения процедуры оценивания	Методы оценивания	Виды выставляемых оценок	Способ учета индивидуальных достижений, обучающихся
1.	Тестирование	1 раз в семестр / письменно	экспертный	По пятибалльной шкале	Электронная система сопровождения обучения СамГТУ
2.	Отчет по лабораторным работам	Систематически на лабораторных занятиях / письменно	экспертный	По пятибалльной шкале	Электронная система сопровождения обучения СамГТУ
3.	Промежуточная аттестация экзамен	по окончании изучения дисциплины/ устно и письменно	экспертный	По пятибалльной шкале	экзаменационная ведомость, зачетная книжка

3.2. Критерии и шкала оценивания результатов изучения дисциплины во время занятий (текущий контроль успеваемости)

Критерии оценки и шкала оценивания теста

Таблица 2

Шкала оценивания	Критерии оценки	Кол-во баллов
«Отлично»	86-100% правильных ответов	17-20 баллов
«Хорошо»	71-85% правильных ответов	14-16 баллов
«Удовлетворительно»	65-70% правильных ответов	12-13 баллов
«Неудовлетворительно»	менее 65% правильных ответов	0-12 баллов

Критерии оценки и шкала оценивания защиты отчёта по лабораторным работам

Таблица 3

Шкала оценивания	Критерии оценки	Кол-во баллов
«Отлично»	ставится, если учащийся выполняет работу в полном объеме с соблюдением необходимой последовательности проведения опытов и измерений; самостоятельно и рационально монтирует необходимое оборудование; все опыты проводит в условиях и режимах, обеспечивающих получение правильных результатов и выводов; соблюдает требования правил безопасности труда; в отчете правильно и аккуратно выполняет все записи, таблицы, рисунки, чертежи, графики, вычисления; правильно выполняет анализ погрешностей. Отвечает на все поставленные вопросы	31-45 баллов
«Хорошо»	ставится, если выполнены требования к оценке «отлично», но было допущено два - три недочета, не более одной негрубой ошибки и одного недочёта	16-30 баллов
«Удовлетворительно»	ставится, если работа выполнена не полностью, но объем выполненной части таков, позволяет получить правильные результаты и выводы: если в ходе проведения опыта и измерений были допущены ошибки. Затрудняется дать ответы на поставленные вопросы	5-15 баллов
«Неудовлетворительно»	ставится, если работа выполнена не полностью	0 баллов

Критерии и шкала оценивания результатов изучения дисциплины на промежуточной аттестации

Основанием для определения оценки на промежуточной аттестации служит уровень освоения обучающимися материала и формирования компетенций, предусмотренных программой учебной дисциплины.

Успеваемость определяется оценками: 5 «отлично»; 4 «хорошо»; 3 «удовлетворительно»; 2 «неудовлетворительно».

Оценку «отлично» получает обучающийся, освоивший компетенции дисциплины на всех этапах их формирования **на 85-100 %,** показавший всестороннее, систематическое и глубокое знание учебного материала, умение свободно выполнять задания, предусмотренные рабочей программой, усвоивший основную и ознакомленный с дополнительной литературой, рекомендованной программой. Как правило, оценка «отлично» выставляется обучающимся, усвоившим взаимосвязь основных положений учебной

дисциплины, необходимых для приобретаемой профессии, проявившим творческие способности в понимании, изложении и использовании учебного материала.

Оценку «хорошо» заслуживает обучающийся, освоивший компетенции дисциплины на всех этапах их формирования **на 71-84 %,** обнаруживший полное знание учебного материала, успешно выполняющий предусмотренные рабочей программой задания, усвоивший основную литературу, рекомендованную в программе. Как правило, оценка «хорошо» выставляется обучающимся, продемонстрировавшим систематическое владение материалом дисциплины, способным к их самостоятельному пополнению и обновлению в ходе дальнейшей учебной работы и профессиональной деятельности, но допустившим несущественные неточности в ответе.

Оценку «удовлетворительно» получает обучающийся, освоивший компетенции дисциплины на всех этапах их формирования **на 51-70 %,** обнаруживший знание основного учебного материала в объёме, необходимом для дальнейшей учебы и предстоящей работы по профессии, справляющийся с выполнением заданий, предусмотренных рабочей программой, знакомый с основной литературой, рекомендованной программой. Как правило, оценка «удовлетворительно» выставляется обучающимся, допустившим погрешности в ответе на экзамене и при выполнении экзаменационных заданий, но обладающим необходимыми знаниями для устранения под руководством преподавателя допущенных недочетов.

Оценка «неудовлетворительно» выставляется обучающемуся, освоившему компетенции дисциплины на всех этапах их формирования менее чем **на 51%,** обнаружившему пробелы в знаниях основного учебного материала, допустившему принципиальные ошибки в выполнении предусмотренных рабочей программой заданий.

Шкала оценивания результатов

Таблица 4

Процентная шкала (при ее использовании)	**Оценка в системе «неудовлетворительно – удовлетворительно – хорошо – отлично»**
0-50%	Неудовлетворительно
51-70%	Удовлетворительно
71-84%	Хорошо
85-100%	Отлично