Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования «Северо-Осетинский государственный университет имени Коста Левановича Хетагурова»

УТВЕРЖДАЮ
Проректор по УР
_____ Л.М. Дигурова
«28» 05 2019 г

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
«Кибербезопасность и интернет-вещей»

Направление подготовки 01.03.01 Математика

Профиль "Кибербезопасность"

Форма обучения – очная

Владикавказ 2019

Программа составлена в соответствии с Федеральным государственным образовательным стандартом высшего образования по направлению подготовки 01.03.01 Математика, утвержденным приказом Министерства образования и науки Российской Федерации от 10.01.2018 г. № 8, учебным планом подготовки бакалавриата по направлению подготовки 01.03.01 Математика, профиль "Кибербезопасность", утвержденным Ученым советом ФГБОУ ВО «СОГУ» от 28.05.2019 г. № 10.

Составитель: доцент Салбиев А.Т.

Рабочая программа обсуждена и утверждена на заседании кафедры алгебры и геометрии.
(протокол №7 от 14.03.2019)

Одобрена советом факультета математики и информационных технологий
(протокол №5 от 29.03.2019)

1. Структура и общая трудоемкость дисциплины

Общая трудоемкость дисциплины составляет 3 зачётные единицы. (108 час.).

	Очная Форма обучения
Курс	4
Семестр	8
Лекции	20
Практические занятия	-
Лабораторные занятия	20
Консультации	-
Итого аудиторных занятий	40
Самостоятельная работа	68
Курсовая работа	-
Зачет	+
Экзамен	-
Общее количество часов	108 час.

2. Цели освоения дисциплины

Целями освоения дисциплины «Кибербезопасность и интернет-вещей» являются изучение:

- основных направлений деятельности по обеспечению безопасности Интернета вещей, киберфизических систем в составе объектов критической информационной инфраструктуры;
- основных понятий в области безопасности Интернета вещей, киберфизических систем в составе объектов критической информационной инфраструктуры (КИИ);
- основных угроз, уязвимостей, рисков в области безопасности Интернета вещей, киберфизических систем в составе объектов критической информационной инфраструктуры;
- технологий угроз сетевой безопасности, а также механизмов противодействия сетевым атакам;
- основных требований нормативно-правовых документов по защите объектов критической информационной инфраструктуры;
- особенностей проектирования систем безопасности объектов критической информационной инфраструктуры.

3. Место дисциплины в структуре ОПОП:

Дисциплина «Кибербезопасность и интернет-вещей» относится к дисциплинам Блок 1. Дисциплины (модули). Часть, формируемая участниками образовательных отношений. Б1.В.07.

Для изучения дисциплины необходимы знания, полученные обучающимися в рамках школьного курса «Информатика», а также в результате освоения дисциплин: «Основы аппаратного и программного обеспечения ПК», «Дискретная математика», «Основы сетевых технологий (CISCO)».

Приступая к изучению дисциплины «Кибербезопасность и интернет-вещей», студент должен иметь представление о базовых понятиях в инфокоммуникационных системах и сетях.

4. Требования к результатам освоения дисциплины

Компетенции обучающегося, формируемые в результате освоения дисциплины.

В результате изучения дисциплины обучающийся должен обладать следующими компетенциями (результатами освоения образовательной программы):

УК-1 -Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач;

ПК-1 -Способен администрировать средства защиты информации в компьютерных системах и сетях.

Взаимосвязь планируемых результатов обучения по дисциплине с формируемыми компетенциями ОПОП:

Компетенции		**Планируемые результаты обучения, соответствующие формируемым компетенциям ОПОП**		
Код	**Формулировка**	**Знать:**	**Уметь**	**Владеть:**
УК-1	Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач	порядок определения источников информации, порядок получения доступа к ним; методы описания и формализации полученной информации; способы верификации получаемой информации; принципы системного подхода; стратегию действий на основе системного подхода, используя обработанную полученную информацию.	использовать способы совершенствования деятельности; умеет использовать способы и приемы самооценки; использовать способы определения приоритетов деятельности	навыками критического анализа проблемных ситуаций;
ПК-1	Способен администрировать средства защиты информации в компьютерных системах и сетях	принципы социальной ответственности; принципы построения профессиональной деятельности и бизнеса;	формировать требований к кибербезопасности (информационной безопасности) систем «Интернета вещей», объектов КИИ; выявлять актуальные	навыками составления практических рекомендаций по использованию результатов научных исследований для

		угрозы и риски для граждан и общества в области безопасности «Интернета вещей» и критической информационной инфраструктуры, ответственность за нарушения требований безопасности.	угрозы кибербезопасности (информационной безопасности) в системах «Интернета вещей» и объектов КИИ, разрабатывать неформализованные модели угроз; разрабатывать неформализованные модели средств, систем и процессов, применяемых в системах «Интернета вещей» и объектов КИИ, анализировать их с точки зрения кибербезопасности (информационной безопасности) и проверять адекватность фактическим средствам, системам и процессам; использовать для построения и проверки моделей пакеты программ анализа и синтеза инфокоммуникационных систем, сетей и устройств	организации работ по исследованию кибербезопасности (информационной безопасности) «Интернета вещей» и объектов КИИ; навыками выполнения работ по обеспечению функционирования систем «Интернета вещей», объектов КИИ в части выполнения требований информационной безопасности (кибербезопасности); навыками управления технологическими изменениями, нахождения путей совершенствования в части модернизации систем кибербезопасности

При проведении учебных занятий обеспечивается развитие у обучающихся навыков командной работы, межличностной коммуникации, принятия решений, лидерских качеств (включая при необходимости проведение интерактивных лекций, групповых дискуссий, ролевых игр, тренингов, анализ ситуаций и имитационных моделей, преподавание дисциплин (модулей) в форме курсов, составленных на основе результатов научных исследований, в том числе с учетом региональных особенностей профессиональной деятельности выпускников и потребностей работодателей).

5. Содержание и учебно-методическая карта дисциплины

Таблица 5.1

Номер недели	Наименование тем (вопросов), изучаемых по данной дисциплине	Занятия			Самостоятельная работа студентов		Формы контроля	Баллы		Литература
		л	пр	лаб	Содержание	Часы		min	max	
1-2	Кибербезопасность: основные понятия и определения. Киберфизические системы и «Интернет-вещей» - соотношение понятий Кибербезопасность (информационная безопасность) киберфизических систем, кибербезопасность в «Интернет-вещей»: основные стандарты, понятия, определения. Киберфизические системы и «Интернет-вещей»: обзор основных проблем, связанных с кибербезопасностью; основные угрозы и уязвимости в сфере кибербезопасности. Регулирование вопросов кибербезопасности в «Интернет- вещей»: международное, в РФ.	2		2	основные требования к специалистам в области кибербезопасности «Интернет-вещей», критической информационной инфраструктуры	8	Конспект, вопросы на коллоквиуме	**0**	**10**	**[1-5]**
3-5	Сетевые технологии и протоколы: основные	3		3	классификация и примеры продуктов «Интернет-вещей»	10	Конспект, вопросы на коллоквиум	**0**	**15**	**[1-5]**

	понятия и определения. Сетевые технологии и протоколы – модель OSI, проблемы безопасности Протоколы связи и аутентификации для киберфизических систем и «Интернет-вещей»: обзор, особенности, проблемы безопасности.				для граждан, примеров угроз, уязвимостей, рисков		е			
6-8	Функциональная безопасность: основные понятия и определения. Функциональная безопасность: основные стандарты, понятия и определения. Обзор основных стандартов в сфере функциональной безопасности.	3		3	основные риски и проблемы кибербезопасности «Интернет-вещей» в сфере здравоохранения	10	Конспект, вопросы на коллоквиуме	**0**	**15**	**[1-5]**
9-11	Кибербезопасность в «Интернет-вещей». Кибербезопасность в «Интернет- вещей» для граждан: классификация продуктов «Интернет- вещей» для граждан, угрозы, уязвимости, риски на примере популярных продуктов. «Интернет-вещей» в сфере	3		3	основные риски и проблемы кибербезопасности для «Умного дома»	10	Конспект, вопросы на коллоквиуме	**0**	**15**	**[1-5]**

	здравоохранения – риски и проблемы. «Умный дом» - риски и проблемы. Юридические инциденты – примеры Цели обеспечения кибербезопасности в «Интернет-вещей» для граждан.									
12-14	Кибербезопасность для систем «Умного города». «Умный город»: 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). «Интернет-вещей» и его применение в Smart Grid, проблемы кибербезопасности	3		3	состав и классификация систем для «Умного города», критериев оценки безопасности, основные угрозы, риски и проблемы, структуры и особенности построения модели угроз	10	Конспект, вопросы на коллоквиуме	**0**	**15**	**[1-5]**
15-16	Кибербезопасность в «Интернет-вещей» в промышленности. Киберфизические системы и «Интернет-вещей» в	3		3	основные риски и проблемы кибербезопасности в Smart Grid	10	Конспект, вопросы на коллоквиуме	**0**	**15**	**[1-5]**

	промышленности: понятие «Индустриальный Интернет-вещей», соотношение с понятием «киберфизическая система», классификация продуктов «Интернет- вещей», соотношение с понятиями АСУТП, ICS; угрозы, уязвимости, риски.									
17-18	Критическая информационная инфраструктура: основные понятия, определения, проектирование систем безопасности. Критическая информационная инфраструктура, основные понятия, стандарты. Критическая информационная инфраструктура РФ, основные понятия, НПА, требования Категорирование объектов КИИ РФ, порядок и критерии Основные подсистемы обеспечения ИБ объектов КИИ. Средства обеспечения кибербезопасности (обзор) Проектирование систем безопасности значимых объектов КИИ	3		3	основные риски и проблемы кибербезопасности в Индустриальном Интернете вещей	10	Конспект, вопросы на коллоквиуме	**0**	**15**	**[1-5]**

	Силы обеспечения кибербезопасности объектов КИИ Требования к специалистам в области кибербезопасности «Интернет-вещей», критической информационной инфраструктуры. Построение СМИБ для объектов КИИ на промышленных объектах: Обзор стандартов семейства ISO / ГОСТ 27К. Состав СМИБ. Особенности создания СМИБ для объектов КИИ на промышленных объектах Ответственность за нарушение требований законодательства РФ в сфере обеспечения безопасности КИИ и КВО ТЭК.									
	ИТОГО	20	0	20		68		**0**	**100**	

Примечания:

– Все виды учебной работы могут проводиться дистанционно на основании локальных нормативных актов.

– В целях реализации индивидуального подхода к обучению студентов, осуществляющих учебный процесс по индивидуальной траектории в рамках индивидуального рабочего плана, изучение данной дисциплины может осуществляться через индивидуальные консультации преподавателя очно, в часы консультаций, по электронной почте и с использованием платформ дистанционного обучения.

6. Образовательные технологии

В соответствии с государственными образовательными стандартами высшего образования реализация учебного процесса должна предусматривать проведение занятий в интерактивных и активных формах. Внедрение этих форм обучения – одно из важнейших направлений совершенствования подготовки студентов в современном вузе. Цель – повышение эффективности образовательного процесса, достижение всеми обучающимися высоких результатов обучения.

Интерактивные формы проведения занятий предполагают обучение в сотрудничестве. Все участники образовательного процесса (преподаватель и студенты) взаимодействуют друг с другом, обмениваются информацией, совместно решают проблемы, моделируют ситуации. Суть использования активных и интерактивных форм проведения состоит в погружении студентов в реальную атмосферу делового сотрудничества по разрешению проблем, оптимальную для выработки навыков и качеств будущего специалиста.

Для решения воспитательных и учебных задач преподавателем могут быть использованы следующие интерактивные формы обучения.

Традиционные лекции и практические (семинарские) занятия с использованием современных интерактивных технологий.

Лекция-диалог – содержание подается через серию вопросов, на которые студент должен отвечать непосредственно в ходе лекции.

Онлайн-семинар – разновидность веб-конференции, проведение онлайн-встреч или презентаций через Интернет в режиме реального времени. Каждый из участников находится у своего компьютера (средства связи), а связь между ними поддерживается через Интернет посредством загружаемого приложения, установленного на компьютере каждого участника.

Видеоконференция – сеанс видеоконференцсвязи (ВКС) – это технология интерактивного взаимодействия двух и более участников образовательного процесса для обмена информацией в реальном режиме времени.

Видео-лекция – снятая на камеру сокращенная лекция, дополненная фотографиями и схемами, иллюстрирующая подаваемый в лекции материал.

Технология электронного обучения (реализуется при помощи электронной образовательной среды СОГУ при использовании ресурсов ЭБС, при проведении автоматизированного тестирования и т. д.).

Творческое задание составляет содержание (основу) любой интерактивной формы проведения занятия. Выполнение творческих заданий требует от студента воспроизведения полученной ранее информации в форме, определяемой преподавателем и требующей творческого подхода: 1) подборка примеров из практики; 2) подборка материала по определенной проблеме;

Публичная презентация проекта - самый эффективный способ донесения важной информации при публичных выступлениях. Слайд-презентации позволяют эффектно и наглядно представить содержание, выделить и проиллюстрировать сообщение.

Интерактивная лекция представляет собой выступление преподавателя перед аудиторий студентов с применением следующих интерактивных форм обучения: 1. управляемая дискуссия или беседа; 2. демонстрация слайдов или учебных фильмов; 3. мозговой штурм; 4. мотивационная речь и др.

Разработка проекта позволяет участникам мысленно выйти за пределы аудитории и составить проект своих действий по обсуждаемому вопросу Участники могут обратиться за консультацией, дополнительной литературой в специализированные учреждения, библиотеки и т.д.

Проблемное обучение - поиск ответов на вопросы по теме.

7. Учебно-методическое обеспечение самостоятельной работы

Самостоятельная работа обучающихся является одним из видов учебных занятий. Самостоятельная работа проводится с целью:

− систематизации и закрепления полученных теоретических знаний и практических умений обучающихся студентов;

− углубления и расширения теоретических знаний;

− формирования умений использовать нормативную, правовую, справочную документацию и специальную литературу;

- формирования самостоятельности мышления, способностей к саморазвитию, самосовершенствованию и самореализации;

− развития исследовательских умений.

К видам самостоятельной работы при изучении данной дисциплины относится: написание докладов, эссе, подготовка презентаций, самостоятельное изучение литературы по теме и составление по ней конспектов, работа со справочными материалами (терминологическими и иными словарями, энциклопедиями) и т.д.

Темы и формы внеаудиторной самостоятельной работы, ее трудоёмкость содержатся в разделе 5, табл. 5.1.

Методические рекомендации по дисциплине прилагаются.

8. Оценочные средства для текущего контроля успеваемости, рубежной аттестации и промежуточной аттестации по итогам освоения дисциплины

Рабочая программа предусматривает проведение лекционных и лабораторных занятий, а также следующие виды работ: самостоятельную работу студентов по подготовке устных сообщений, написанию докладов, подготовку презентаций и обсуждений по темам дисциплины - работу в активной и интерактивной формах.

Рабочая программа предполагает текущий и промежуточный контроль знаний.

Текущий контроль – это непрерывно осуществляемый мониторинг уровня усвоения знаний и формирования умений и навыков в течение семестра или учебного года. Текущий контроль знаний, умений и навыков студентов осуществляется в ходе учебных (аудиторных) занятий, проводимых по расписанию. Формами текущего контроля выступают опросы на занятиях с целью проверки наличия знаний, необходимых для усвоения нового материала или для выяснения степени усвоения изложенного материала.

Рубежный контроль осуществляется по окончании изучения материала модуля в заранее установленное время. Рубежный контроль проводится с целью определения качества усвоения материала учебного модуля в целом. В течение семестра такие контрольные мероприятия проводятся по графику.

Контрольные задания (демоверсии) для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

1. Состав и классификация систем для «Умного города», критерии оценки безопасности, основных угроз, рисков и проблем, структуры и особенностей построения модели угроз;
2. Основные требования к специалистам в области кибербезопасности «Интернет-вещей», критической информационной инфраструктуры .

Критерии оценивания представлены в таблице 8.1.

Примеры тестовых заданий по дисциплине:
Вы в одном шаге от окончания курса — остался решающий экзамен. Он охватит темы всех модулей.

1. Какой из списков решений относится к индустриальному интернету вещей?
   - Мониторинг открытия канализационных люков, автоматизированный магазин без кассиров и продавцов, счетчики воды в домах, которые автоматически передают показания в ЕИРЦ.
   - «Умная» домашняя колонка от Amazon, Яндекс или Google, автополив домашних растений, фитнес-прибор, который следит за правильной осанкой человека.
2. Какой термин не существовал до появление интернета вещей?
   - АСКУЭ
   - АСУТП
   - Вавиот
3. Вас просят помочь с выбором датчика влажности для теплиц: задача состоит в том, чтобы замерять уровень влаги и в почве, и в воздухе, а при сильном падении или разнице уровней включать систему орошения. Что вы посоветуете?
   - Датчик AM2302 DHT22
   - Датчик CCS811 HDC1080
   - Датчик RS485
   - Посоветую подключить к обсуждению инженера: данных мало, выбор датчиков большой
4. Какой из элементов умного замка, который открывается благодаря Bluetooth-команде с телефона, не обязателен?
   - Датчик
   - Актуатор (Исполнительное устройство)
   - Батарея или иной источник питания
   - Микроконтроллер
   - Радиомодуль
5. Вы уже знаете, что в зависимости от задачи мы можем добавлять и убирать из устройства какие-то компоненты. Но без каких трех элементов точно невозможно представить наше устройство в системе интернета вещей?
   - Батарея или иной источник питания, микроконтроллер, радиомодуль.
   - Датчик, актуатор (исполнительное устройство), батарея или иной источник питания.
   - Актуатор (Исполнительное устройство), батарея или иной источник питания, микроконтроллер.
6. Представьте, что вам нужно подключить готовое устройство, электронный термостат, к интернету вещей, чтобы собирать информацию о температуре воды в трубах, идущих в подвале дома. Что нужно добавить к нему?
   - микроконтроллер
   - питание
   - исполнительное устройство (актуатор)
   - wifi-роутер
7. Какой из этих факторов нужно учитывать при выборе датчика в первую очередь?
   Энергоэффективность
   - Габариты (размеры)
   - Точность измерений

- Диапазон измерений
- Все факторы нужно учесть

8. В теплице стоят приборы-гигрометры — они выводят уровень влажности на ЖК-дисплеях, встроенных в их корпуса, а сотрудники раз в час обходят территорию и заносят показания в электронный журнал. Можно ли улучшить эту систему?

- Нет, ведь данные уже собираются и оцифровываются.
- Да, можно улучшить процесс записи данных.

9. Что такое микроконтроллер?

- Переключатель режимов работы и тока в устройстве.
- Небольшой компьютер, который управляет устройством в интернете вещей.
- Прибор, который обеспечивает связь устройства с сервером.

10. Датчики метана отправляют данные о содержании газа в воздухе каждые 5 минут, независимо от того, превышен он или нет. Нужно перепрограммировать систему так, чтобы сигнал поступал только в случае опасности. На каком уровне системы эффективнее изменить программу?

- На уровне микроконтроллера
- На уровне сервера
- На уровне платформы

11. Как лучше защитить всю систему интернета вещей?

Написать и использовать свою систему шифрования данных на всех этапах их передачи.

- Скачать и установить антивирусы на всех устройства, базовые станции и серверы.
- Обратиться к специалистам по кибербезопасности и заказать комплекс услуг у них.

12. Мы оснастили батареи в больнице новыми электронными термостатами. Они отслеживают и передают температуру воздуха возле каждой точки установки — если воздух вокруг достаточно прогрелся, на термостат поступает команда перекрыть батарею до момента, пока температура не опустится ниже нормы. Как злоумышленник может навредить нашей системе, если мы не защитили ее достаточно хорошо?

- Подключиться к термостату и отправлять с него ложные данные о температуре.
- Подключиться к серверу и отправить команду всем термостатам на перекрытие батареи.
- Подключиться к термостату и отдать команду перекрыть конкретную батарею.
- Перехватывать и подделывать сигналы, добавлять в систему ложные термостаты, выводить на платформе неверные данные.
- Злоумышленник может сделать абсолютно все вышеперечисленное.

13. Что из этого — названия платформ интернета вещей? Если вы не уверены, поищите ответ в интернете.

- Amazon Prime, Zigbee
- Bluetooth, DecaWave, Яндекс.Облако
- Microsoft Azure, IBM Bluem

Методика формирования результирующей оценки

Таблица 8.1

Этап	**Форма контроля**	**Критерии оценивания (процент от максимального кол-ва баллов)**			
		86-100 %	**71–85%**	**60–70%**	**Менее 60%**
1. Текущий контроль (max 25 баллов за 1 модуль)					
		7-8 баллов	6–7 баллов	4–5 баллов	0–3 баллов
	Посещение занятий (max 8 б.)	Студент посетил более 85% занятий	Студент посетил 71–85% занятий	Студент посетил 56–70% занятий	Студент посетил менее 56% занятий

		9–10 баллов	7–8 баллов	6–7 баллов	0–5 баллов
	Текущая работа в течение модуля (max 10б.)	Студент активно работает на занятиях, превосходно выполняет все задания преподавателя.	Студент активно работает на занятиях, хорошо выполняет задания преподавателя.	Студент недостаточно активно работает на занятиях, удовлетворительно выполняет задания преподавателя.	Студент недостаточно активно работает на занятиях, неудовлетворительно выполняет задания преподавателя.
		3/2 балла	2 балла	1 балл	0 баллов
	Доклад, презентация (max 3б.) / опорный конспект (max 2б.)	Тема полностью раскрыта. Превосходное владение материалом. Высокий уровень самостоятельности, логичности, аргументированности. Превосходный стиль изложения.	Тема в основном раскрыта. Хорошее владение материалом. Средний уровень самостоятельности, логичности, аргументированности. Хороший стиль изложения.	Тема частично раскрыта. Удовлетворительное владение материалом. Низкий уровень самостоятельности, логичности, аргументированности. Удовлетворительный стиль изложения.	Тема не раскрыта. Неудовлетворительное владение материалом. Недостаточный уровень самостоятельности, логичности, аргументированности. Неудовлетворительный стиль изложения.
2. Рубежный контроль (25б. за 1 модуль)					
		22–25 баллов	18–21 балл	14–17 баллов	0–13 баллов
	Контрольная работа	Правильно выполнены все задания. Продемонстрирован высокий уровень владения материалом. Проявлены превосходные способности применять знания и умения к выполнению конкретных заданий.	Правильно выполнена большая часть заданий. Присутствуют незначительные ошибки. Продемонстрирован хороший уровень владения материалом. Проявлены средние способности применять знания и умения к выполнению конкретных заданий.	Задания выполнены более чем наполовину. Присутствуют серьезные ошибки. Продемонстрирован удовлетворительный уровень владения материалом. Проявлены низкие способности применять знания и умения к выполнению конкретных заданий.	Задания выполнены менее чем наполовину. Продемонстрирован неудовлетворительный уровень владения материалом. Проявлены недостаточные способности применять знания и умения к выполнению конкретных заданий.
3. Итоговый контроль по дисциплине					
		43–50 баллов	36–42 балла	28–35 баллов	0–27 баллов
	Экзамен/зачет	Дан полный, развернутый ответ на поставленный вопрос. Ответ формулируется в терминах науки, изложен литературным языком, логичен, доказателен, демонстрирует авторскую позицию студента.	Дан полный ответ на поставленный вопрос, показано умение выделить существенные и несущественные признаки, причинно-следственные связи. Но допущены незначительные ошибки, исправленные студентом с помощью	Дан недостаточно полный ответ. Студент не способен самостоятельно выделить существенные и несущественные признаки и причинно-следственные связи. Речевое оформление требует поправок, коррекции.	Не получены ответы по базовым вопросам дисциплины или дан неполный ответ и допущены грубые ошибки. Речь неграмотная. Уточняющие вопросы преподавателя не приводят к коррекции ответа студента не только на поставленный вопрос, но и на

			«наводящих» вопросов преподавателя.		другие вопросы дисциплины.

Студенты, получившие в ходе текущего и рубежного контроля 56-100 баллов, автоматически получают «Зачет» или соответствующую шкале экзаменационную оценку. Результирующая оценка складывается по соответствующей БРС формуле.

Вопросы для подготовки к зачёту:

- основные понятия в области кибербезопасности Интернета вещей; основные угрозы, риски и уязвимости в сфере кибербезопасности Интернета вещей и критической информационной инфраструктуры;
- основные протоколы передачи данных и аутентификации, используемые в «Интернет вещей»;
- основные понятия в сфере функциональной безопасности;
- положения основных нормативных актов, регулирующих сферу безопасности критической информационной инфраструктуры Российской Федерации;
- архитектура основных подсистем обеспечения ИБ объектов КИИ;
- основные определения СМИБ и особенности построения СМИБ для объектов КИИ на промышленных объектах;
- положения нормативных актов, устанавливающих ответственность за нарушение требований законодательства РФ в сфере обеспечения безопасности КИИ и КВО ТЭК.
- основные средства обеспечения кибербезопасности (архитектура, принципы построения);
- принципы проектирования систем безопасности значимых объектов КИИ;
- состав и способы организации деятельности сил обеспечения кибербезопасности объектов КИИ;
- основные требования к специалистам в области кибербезопасности «Интернет-вещей», критической информационной инфраструктуры;
- цели обеспечения кибербезопасности в «Интернет-вещей» для граждан;
- классификация и примеры продуктов «Интернет-вещей» для граждан, примеры угроз, уязвимостей, рисков;
- основные риски и проблемы кибербезопасности «Интернет-вещей» в сфере здравоохранения;
- основные риски и проблемы кибербезопасности для «Умного дома»;
- состав и классификация систем для «Умного города», критерии оценки безопасности, основных угроз, рисков и проблем, структуры и особенностей построения модели угроз;
- основные риски и проблемы кибербезопасности в Smart Grid;
- основные риски и проблемы кибербезопасности в Индустриальном Интернете вещей;
- примеры юридических инцидентов в области регулирования кибербезопасности «Интернета-вещей».

Показатели и критерии оценивания компетенций на различных этапах их формирования, описание шкал оценивания

Уровень сформированности компетенций

«Минимальный уровень не достигнут» (менее 56 баллов)	«Минимальный уровень» (56-70 баллов)	«Средний уровень» (71-85 баллов)	«Высокий уровень» (86-100 баллов)
Компетенции не сформированы. Знания отсутствуют, умения и навыки не сформированы.	*Компетенции сформированы.* Сформированы базовые структуры знаний. Умения фрагментарны и носят репродуктивный характер. Демонстрируется низкий уровень самостоятельности практического навыка.	*Компетенции сформированы.* Знания обширные, системные. Умения носят репродуктивный характер, применяются к решению типовых заданий. Демонстрируется достаточный уровень самостоятельности устойчивого практического навыка.	*Компетенции сформированы.* Знания твердые, аргументированные, всесторонние. Умения успешно применяются к решению как типовых, так и нестандартных творческих заданий. Демонстрируется высокий уровень самостоятельности, высокая адаптивность практического навыка
Описание критериев оценивания			
Обучающийся демонстрирует: - существенные пробелы в знаниях учебного материала; - допускаются принципиальные ошибки при ответе на основные вопросы, отсутствует знание и понимание основных понятий и категорий; -непонимание сущности дополнительных вопросов в рамках заданий; - отсутствие умения выполнять практические задания, предусмотренные программой дисциплины; - отсутствие готовности (способности) к дискуссии и низкую степень контактности.	Обучающийся демонстрирует: - знания теоретического материала; - неполные ответы на основные вопросы, ошибки в ответе, недостаточное понимание сущности излагаемых вопросов; - неуверенные и неточные ответы на дополнительные вопросы; - недостаточное владение литературой, рекомендованной программой дисциплины; - умение без грубых ошибок решать практические задания, которые следует выполнить.	Обучающийся демонстрирует: - знание и понимание основных вопросов контролируемого объема программного материала; - твердые знания теоретического материала. -способность устанавливать и объяснять связь практики и теории, выявлять противоречия, проблемы и тенденции развития; - правильные и конкретные, без грубых ошибок, ответы на поставленные вопросы; - умение решать практические задания, которые следует выполнить; - владение основной литературой, рекомендованной программой дисциплины; - наличие собственной	Обучающийся демонстрирует: - глубокие, всесторонние и аргументированные знания программного материала; - полное понимание сущности и взаимосвязи рассматриваемых процессов и явлений, точное знание основных понятий в рамках обсуждаемых заданий; - способность устанавливать и объяснять связь практики и теории; - логически последовательные, содержательные, конкретные и исчерпывающие ответы на все задания, а также дополнительные вопросы экзаменатора; - умение решать практические задания; - свободное использование в

		обоснованной позиции по обсуждаемым вопросам. Возможны незначительные оговорки и неточности в раскрытии отдельных положений вопросов, присутствует неуверенность в ответах.	ответах на вопросы материалов рекомендованной основной и дополнительной литературы.
Оценка «неудовлетворительно» /не зачтено	**Оценка «удовлетворительно» / «зачтено»**	**Оценка «хорошо» / «зачтено»**	**Оценка «отлично» / «зачтено»**

9. Учебно-методическое и информационное обеспечение дисциплины

а) основная литература:

1. Дубков, И.С. Решение практических задач на базе технологии интернета вещей : учебное пособие : [16+] / И.С. Дубков, П.С. Сташевский, И.Н. Яковина ; Новосибирский государственный технический университет. – Новосибирск : Новосибирский государственный технический университет, 2017. – 80 с. : ил.,табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=576635 – Библиогр. в кн. – ISBN 978-5-7782-3161-0. – Текст : электронный.
2. Изотов, И.Н. Разработка системы интернета вещей «Свежий воздух»: выпускная квалификационная работа / И.Н. Изотов ; Уральский федеральный университет им. первого Президента России Б. Н. Ельцина, Институт радиоэлектроники и информационных технологий – РтФ, Школа бакалавриата. – Екатеринбург : б.и., 2019. – 66 с. : ил., табл., схем. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=563483 – Текст : электронный.
3. Колесников, М.В. Исследование и разработка интеллектуальных контроллеров для промышленного интернета вещей: выпускная квалификационная работа / М.В. Колесников ; Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики, Факультет СуиР. – Санкт-Петербург : б.и., 2019. – 62 с. : ил., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=562997 – Текст : электронный.

б) дополнительная литература:

4. Беспроводные технологии / гл. ред. П. Правосудов ; учред. ООО «Издательство Файнстрит», Г.А. Дружинина. – Санкт-Петербург : Медиа КиТ, 2015. – № 4(41). – 68 с. : ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=430233. – ISSN 2079-9233. – Текст : электронный.
5. Филимонова, А.А. Разработка ПО, обеспечивающего безопасность помещения с помощью «умных вещей» / А.А. Филимонова ; Амурский государственный университет (АмГУ). – Благовещенск : б.и., 2020. – 66 с. : ил., табл., схем – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=596766 – Текст : электронный.

в) электронные библиотечные системы, с которыми у СОГУ имеется действующий договор, современные профессиональные базы, информационные справочные системы:

– eLIBRARY.RU [Электронный ресурс]: научная электронная библиотека. – URL: http://www.elibrary.ru.

– База данных «ЭБС elibrary»: http://elibrary.ru

– Издательство «Юрайт» [Электронный ресурс]: электронно-библиотечная система. – URL: http://biblio-online.ru.

- Университетская библиотека online [Электронный ресурс]: электронно-библиотечная система. – URL: http://www.biblioclub.ru.

10. Материально-техническое обеспечение дисциплины

Занятия по дисциплине проводятся в аудиториях, обеспеченных компьютерами, имеющими доступ к сети Интернет, интерактивными досками и мультимедийным оборудованием.

Лицензионное программное обеспечение:

1. Windows 10 Pro for Workstations, (№ 4100072800 Microsoft Products (MPSA) от 04.2016г);
2. Office Standard 2016 (№ 4100072800 Microsoft Products (MPSA) от 04.2016г);
3. Система поиска текстовых заимствований «Антиплагиат ВУЗ»;

Перечень ПО в свободном доступе:

1. Kaspersky Free;
2. WinRar;
3. Google Chrome;
4. Yandex Browser;
5. OperaBrowser;
6. VisualStudioCode;
7. Blend for Visual Studio;
8. Visual Studio 2019.

11. Лист обновления/актуализации

1. Рабочая программа

пересмотрена и актуализирована на заседании кафедры алгебры и геометрии протокол № 7 от 24.03.2020г.;

одобрена на заседании совета факультета математики и информационных технологий, протокол № 5 от 27.03.2020 г.