МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ СИСТЕМ УПРАВЛЕНИЯ И РАДИОЭЛЕКТРОНИКИ»
(ТУСУР)

АННОТАЦИЯ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

Безопасность интернета вещей

Уровень образования: **высшее образование - специалитет**
Направление подготовки / специальность: **10.05.02 Информационная безопасность телекоммуникационных систем**
Направленность (профиль) / специализация: **Защита информации в системах связи и управления**
Форма обучения: **очная**
Факультет: **ФБ, Факультет безопасности**
Кафедра: **БИС, Кафедра безопасности информационных систем**
Курс: **5**
Семестр: **10**
Учебный план набора 2020 года

Распределение рабочего времени

№	Виды учебной деятельности	10 семестр	Всего	Единицы
1	Лекции	18	18	часов
2	Практические занятия	28	28	часов
3	Всего аудиторных занятий	46	46	часов
4	Самостоятельная работа	26	26	часов
5	Всего (без экзамена)	72	72	часов
6	Общая трудоемкость	72	72	часов
		2.0	2.0	З.Е.

Зачёт: 10 семестр

Томск

1. Цели и задачи дисциплины

1.1. Цели дисциплины

Целью изучения данной дисциплины является изучение:

основных направлений деятельности по обеспечению безопасности систем Интернета вещей;

основных понятий в области безопасности Интернета вещей;

основных угроз, уязвимостей, рисков в области безопасности Интернета вещей;

технологий угроз сетевой безопасности, а также механизмов противодействия сетевым атакам;

основных требований нормативно-правовых документов по защите объектов критической информационной инфраструктуры.

1.2. Задачи дисциплины

– научить студентов разрабатывать архитектуру систем «Интернета вещей», принимать решения по выбору используемых протоколов, технологий и архитектурных компонентов системы;

– научить студентов анализировать риски в области безопасности систем «Интернета вещей»;

– научить студентов применять на практике полученные знания для противодействия сетевым атакам на системы «Интернет вещей».

2. Место дисциплины в структуре ОПОП

Дисциплина «Безопасность интернета вещей» (Б1.В.03.01) относится к блоку 1 (вариативная часть).

Предшествующими дисциплинами, формирующими начальные знания, являются: Безопасность операционных систем, Безопасность сенсорных систем, Безопасность сетевых протоколов высокого уровня, Безопасность сетевых протоколов низкого уровня, Безопасность систем баз данных, Защита информации в компьютерных сетях, Защита информации в системах беспроводной связи, Информационная безопасность телекоммуникационных систем, Основы информационной безопасности, Сети и системы передачи информации, Технологии Интернета вещей.

3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

– ПК-3 способностью оценивать технические возможности и вырабатывать рекомендации по построению телекоммуникационных систем и сетей, их элементов и устройств;

– ПК-14 способностью выполнять установку, настройку и обслуживание, диагностику, эксплуатацию и восстановление работоспособности телекоммуникационного оборудования и приборов, технических и программно-аппаратных средств защиты телекоммуникационных сетей и систем;

– ПК-15 способностью проводить инструментальный мониторинг защищенности телекоммуникационных систем, обеспечения требуемого качества обслуживания;

В результате изучения дисциплины обучающийся должен:

– **знать** способы формирования требований обеспечения информационной безопасности систем «Интернета вещей»; основные положения стандартов по функциональной безопасности АСУ ТП («Индустриального Интернета вещей»); требования НПА и стандартов по разработке моделей угроз информационной безопасности; существующие технологии в области "Интернета Вещей"; основные тренды и направления в области "Интернета Вещей"; наиболее распространенные уязвимости IoT-устройств и протоколов передачи данных; средства обеспечения информационной безопасности IoT-систем; основные нормативно правовые акты и нормативные методические документы в области инфокоммуникационных систем; принципы построения защищенных телекоммуникационных систем; механизмы реализации атак в сетях интернета вещей; защитные механизмы и средства обеспечения сетевой безопасности; средства и методы предотвращения и обнаружения вторжений.

– **уметь** обнаруживать типовые уязвимости IoT-систем; разбираться в существующих IoT-технологиях и применять их к конкретным сценариям; внедрять типовые решения по информационной безопасности IoT-систем; осуществлять меры противодействия нарушениям сетевой без-

опасности с использованием различных программных и аппаратных средств защиты в соответствии с требованиями нормативно правовых актов и нормативных методических документов; проводить анализ защищенности IoT-систем.

– **владеть** терминологией в области безопасности систем интернета вещей; базовыми навыками по объединению конечных устройств в сеть; навыками реализации сетевых протоколов с помощью программных средств; навыками применения нормативно правовых актов и нормативных методических документов в области инфокоммуникационных систем; методами защиты информации в IoT-системах; инструментами анализа защищенности IoT-систем; методикой анализа результатов работы средств обнаружения вторжений.

4. Название разделов (тем) дисциплины

Названия разделов дисциплины
10 семестр
1 Интернет вещей: технологии, рынок, развитие
2 Угрозы безопасности интернета вещей
3 Безопасность и стандартизация в сфере интернета вещей