

БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

УТВЕРЖДАЮ

Проректор по учебной работе и
образовательным инновациям

О.И. Чуприс

РБ 
Регистрационный № УД- 5815 /уч.

ТЕХНОЛОГИИ И БЕЗОПАСНОСТЬ ИНТЕРНЕТА ВЕЩЕЙ

Учебная программа учреждения высшего образования
по учебной дисциплине для специальности

1-98 01 01 Компьютерная безопасность (по направлениям)
Направление специальности 1-98 01 01-02 Компьютерная безопасность
(радиофизические методы и программно-технические средства)

2018 г.

Учебная программа составлена на основании ОСВО 1-98 01 01-2013 и учебного плана Р 98 – 139/уч.2013

СОСТАВИТЕЛЬ:

К.С. Мулярчик, доцент кафедры телекоммуникаций и информационных технологий Белорусского государственного университета, кандидат технических наук

РЕКОМЕНДОВАНА К УТВЕРЖДЕНИЮ:

Кафедрой телекоммуникаций и информационных технологий факультета радиофизики и компьютерных технологий Белорусского государственного университета (протокол № 3 от 16.10.2018 г.)

Учебно-методической комиссией факультета радиофизики и компьютерных технологий Белорусского государственного университета (протокол № 2 от 23.10.2018 г.)

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Учебная дисциплина «Технологии и безопасность интернета вещей» посвящена изучению принципов построения и функционирования телекоммуникационных систем класса «Интернет вещей», а также практическому использованию данных систем в различных отраслях экономики и сферах жизнедеятельности человека.

При изучении учебной дисциплины рассматриваются такие темы, как: основные положения и архитектура систем «Интернет вещей», ведущие игроки на рынке систем «Интернета вещей», «Интернет вещей» в различных сферах деятельности и отраслях экономики, технологии «Интернета вещей». В процессе обучения акцент делается на комплексном и всестороннем освоении данных тем, при котором затрагиваются как технические, так и бизнес аспекты.

Целью изучения данной дисциплины является формирование у слушателей начального навыка проектирования, разработки и внедрения систем «Интернет вещей».

Задачи учебной дисциплины:

- изучить базовые фундаментальные понятия, принципы построения и основные структурные элементы систем «Интернета вещей»,
- научить студентов формировать требования к системам «Интернета вещей» и разрабатывать технические задания,
- научить студентов разрабатывать архитектуру систем «Интернета вещей», принимать решения по выбору используемых протоколов, технологий и архитектурных компонентов системы,
- научить студентов анализировать и разрабатывать бизнес-модели предоставления услуг и организации сервисов с использованием систем «Интернета вещей»,
- научить студентов применять на практике полученные знания для управления проектами по разработке и внедрению систем «Интернет вещей».

Для успешного усвоения учебной дисциплины необходимы знания по дисциплинам «Основы радиоэлектроники», «Компьютерные сети», «Микропроцессоры и аппаратные средства вычислительной техники», «Распределенные вычислительные системы и облачные технологии», «Системы связи и сети передачи информации», «Интеллектуальный анализ данных». Знания, полученные в рамках учебной дисциплины «Технологии и безопасность интернета вещей» дают базу, необходимую для успешного изучения учебной дисциплины «Программно-аппаратные средства обеспечения информационной безопасности».

В результате изучения учебной дисциплины студент должен:

знать:

- принципы построения, технологии и варианты использования систем «Интернета вещей»;
- основные протоколы организации взаимодействия между устройствами систем «Интернет вещей»;

уметь:

- разрабатывать концепции и архитектуру прикладных систем «Интернета вещей»;
- применять основные протоколы и технологии «Интернета вещей» при построении соответствующих систем;

владеть:

- основными подходами к проектированию концепции и архитектуры систем «Интернета вещей».

Состав компетенций специалиста

Требования к академическим компетенциям специалиста:

- АК-1- уметь применять базовые научно - теоретические знания для решения теоретических и практических задач;
- АК-4- уметь работать самостоятельно;
- АК-5- быть способным выработать новые идеи (креативность);
- АК-6- владеть междисциплинарным подходом при решении проблем;
- АК-7- иметь навыки, связанные с использованием технических устройств, управлением информацией и работой с компьютером.

Требования к социально-личностным компетенциям специалиста:

- СЛК-3- обладать способностью к межличностным коммуникациям;
- СЛК-5- быть способным к критике и самокритике (критическое мышление);
- СЛК-6- уметь работать в команде.

Требования к профессиональным компетенциям специалиста:

- ПК-3- разрабатывать модели явлений, процессов или систем при организации защиты информации;
- ПК-4- выбирать необходимые методы исследования, модифицировать существующие, разрабатывать новые методы и применять их для решения поставленных задач при организации защиты информации;
- ПК-5- выполнять оценку эффективности защиты информации;
- ПК-6- работать с юридической литературой и трудовым законодательством;
- ПК-9- анализировать и оценивать собранные данные;
- ПК-10- вести переговоры, разрабатывать контракты с другими заинтересованными участниками;
- ПК-15- организовывать процесс создания, оценки и эксплуатации средств и систем защиты информации, поддерживать и повышать их безопасность, осуществлять контроль за их использованием.

На изучение дисциплины в 8 семестре отводится всего 116 часов, из них аудиторные - 62 часа: 34 часа – лекции, 28 часов – лабораторные работы. Число зачетных единиц – 3,5.

Форма текущей аттестации – зачет в восьмом семестре.

Форма получения образования – очная.

СОДЕРЖАНИЕ УЧЕБНОГО МАТЕРИАЛА

Тема 1. Введение в «Интернет вещей». Основные положения.

«Интернет вещей» как одна из ключевых технологий современного цифрового общества и экономики. Эволюция коммуникационных и вычислительных технологий, появление «Интернета вещей». Типичные сценарии использования систем «Интернет вещей» для компаний и частных лиц. Место «Интернета вещей» в цепочке создания ценности. «Интернет вещей» и изменение бизнес-процессов, подходов и технологий осуществления операционной деятельности компании. Взаимосвязь людей, процессов, данных и предметов, «Всеобъемлющий Интернет» («Internet of Everything»). Технологии, тесно связанные с «Интернетом вещей»: большие данные, машинное обучение.

Архитектура систем «Интернета вещей». Основные требования к системам «Интернета вещей». Основные характеристики аппаратного обеспечения систем «Интернета вещей»: доступность по сетевому адресу, низкое энергопотребление, долгое время жизни, миниатюризация, система на кристалле, «интеллектуализация» устройства и использование высокоуровневых языков программирования. Выбор сценария функционирования систем «Интернета вещей» в зависимости от предъявляемых требований, примеры. Понятие «межмашинного взаимодействия». Использование «Интернета вещей» для организации межмашинного взаимодействия. Развертывание систем «Интернета вещей».

Ведущие игроки на рынке систем «Интернета вещей». Обзор существующих платформ «Интернета вещей»: Amazon AWS IoT, Microsoft Azure IoT, Cisco Jasper IoT, GE Predix, PTC ThingWorx, Watson IoT. Примеры.

Тема 2. «Интернет вещей» в различных сферах деятельности и отраслях экономики.

Организация предоставления услуг на базе «Интернета вещей». Потребительский и промышленный «Интернет вещей». Основные типы компаний в цепочке создания ценности: производители оборудования и разработчики платформ, провайдеры услуг. Монетизация услуг на базе «Интернета вещей». Основные бизнес-модели.

«Интернет вещей» в автомобильной и транспортной отраслях. Основные сценарии использования «Интернета вещей». Подключенный автомобиль и соответствующая экосистема. Платформа Mojio. Кейс-стади SAP, Hertz и Nokia. Перспективные направления использования «Интернета вещей» в автомобильной отрасли: техническое обслуживание, страхование, аренда автомобилей, путешествия и туризм, мониторинг и управление трафиком. «Интернет вещей» в логистике.

«Интернет вещей» в промышленности и производстве. «Индустриальный

интернет вещей». Прогностическое обслуживание. Интеграция систем «Интернета вещей» с корпоративными ERP системами.

«Умный город». «Умное здание». «Интернет вещей» в здравоохранении. «Интернет вещей» в энергетике. «Интернет вещей» в розничной торговле. «Интернет вещей» в сельском хозяйстве. Другие сферы применения «Интернета вещей».

Тема 3. Технологии «Интернета вещей»

Технологии беспроводных сетей с низким энергопотреблением (LPWAN, WLAN, WPAN). Сети LoRa/LoRaWAN, SIGFOX, "Стриж". Использование сетей сотовой связи для «Интернета вещей», технологии EC-GSM, LTE-M, NB-IoT. «Интернет вещей» в универсальных сетях 5G. Беспроводные сенсорные сети на основе технологий Z-Wave, ZigBee, BLE 4.2 (Bluetooth Mesh). Стандарт IEEE 802.15.4. Стек протоколов 6LoWPAN. Стандарт Wi-Fi HaLow (спецификация IEEE 802.11ah).

Протоколы прикладного уровня для «Интернета вещей»: CoAP, MQTT, XMPP, AMQP, JMS, REST/HTTP. Архитектура систем на основе протокола MQTT. Брокеры. Схема «публикация/подписка». Протоколы управления "умными" устройствами: LWM2M, CWMP, OMA-DM.

Аппаратное обеспечение «Интернета вещей». Технологии «умных устройств». Специализированные операционные системы. MongooseOS. Система на кристалле ESP32. Технология OTA (Over-the-air-update). Облачные вычисления в «Интернете вещей». Концепция «туманных вычислений».

Тема 4. Безопасность и стандартизация в сфере «Интернета вещей»

Основные тенденции в сфере безопасности «Интернета вещей». Подходы к обеспечению комплексной информационной и функциональной безопасности систем «Интернета вещей» на протяжении их жизненного цикла.

Анализ угроз для систем «Интернета вещей». Модель злоумышленника. Классификация уязвимостей в «Интернете вещей» по версии OWASP и IoT Attack Surface Areas Project. Анализ уязвимостей в существующих платформах «Интернет вещей».

Принципы обеспечения безопасности в системах «Интернета вещей»: на уровне устройств и шлюзов, сети и транспорта, приложений. Криптографические механизмы и протоколы, адаптированные под устройства с ограниченными вычислительными возможностями.

Стандартизация в сфере «Интернета вещей». Существующие рабочие стандарты организаций IEEE, ISO/IEC и др. Стандарт ISO/IEC 30141 "Internet of Things Reference Architecture (IoT-RA)". Стандарты для "умного дома".

УЧЕБНО-МЕТОДИЧЕСКАЯ КАРТА

Номер раздела, темы, занятия	Название раздела, темы	Количество аудиторных часов					Количество часов УСП	Формы контроля знаний
		Лекции	Практические занятия	Семинарские занятия	Лабораторные занятия	Иное		
1	2	3	4		5	6	8	9
1.	Тема 1. Введение в «Интернет вещей». Основные положения	6						реферат
1.1.	«Интернет вещей» как одна из ключевых технологий современного цифрового общества и экономики. Архитектура систем «Интернета вещей».	6			4			отчет по лабораторной работе с их устной защитой
2.	Тема 2. «Интернет вещей» в различных сферах деятельности и отраслях экономики	12						реферат
2.1.	Основные бизнес-модели.	4						
2.2.	«Интернет вещей» в автомобильной и транспортной отраслях.	4			4			отчет по лабораторной работе с их устной защитой
2.3.	«Интернет вещей» в промышленности и производстве.	4			4			отчет по лабораторной работе с их устной защитой
3.	Тема 3. Технологии «Интернета вещей»	12						реферат

3.1.	Технологии беспроводных сетей с низким энергопотреблением (LPWAN, WLAN, WPAN).	4			4			отчет по лабораторной работе с их устной защитой
3.2.	Протоколы прикладного уровня для «Интернета вещей». MQTT.	4			4			отчет по лабораторной работе с их устной защитой
3.3.	Аппаратное обеспечение «Интернета вещей».	4			4			отчет по лабораторной работе с их устной защитой
4.	Тема 4. Безопасность и стандартизация в сфере «Интернета вещей»	4						реферат
4.1.	Принципы обеспечения безопасности в системах «Интернета вещей». Стандартизация в сфере «Интернета вещей».	4			4			отчет по лабораторной работе с их устной защитой
	Итого	34			28			

ИНФОРМАЦИОННО-МЕТОДИЧЕСКАЯ ЧАСТЬ

Перечень литературы:

Основная

1. Грингард С., Интернет вещей. Будущее уже здесь / С. Грингард // М.: Альпина Паблишер. – 2016. – 188 с.

Дополнительная

1. Нестеров С.А. Основы информационной безопасности. Учебник и практикум – М.: Изд-во “Юрайт”, 2017 - 322 с.

Примерный перечень лабораторных работ

1. Аппаратное обеспечение «Интернета вещей». Разработка технического задания на создание «умного» устройства
2. Разработка архитектуры проекта. Разработка бизнес-модели реализации проекта.
3. Изготовление прототипа устройства
4. Тестирование прототипа устройства
5. Разработка презентации и представление прототипа устройства

Перечень используемых средств диагностики

Для контроля качества обучения используются следующие средства диагностики:

- отчеты по лабораторным работам с их устной защитой;
- реферат

Методика формирования итоговой оценки

Итоговая оценка формируется на основе:

1. Правил проведения аттестации студентов (Постановление Министерства образования Республики Беларусь № 53 от 29 мая 2012 г.);
2. Положения о рейтинговой системе оценки знаний по дисциплине в БГУ (Приказ ректора БГУ от 18.08.2015 № 382-ОД;
3. Критериев оценки знаний студентов (письмо Министерства образования от 22.12.2003 г.)

ПРОТОКОЛ СОГЛАСОВАНИЯ УЧЕБНОЙ ПРОГРАММЫ УВО

Название учебной дисциплины, с которой требуется согласование	Название кафедры	Предложения об изменениях в содержании учебной программы учреждения высшего образования по учебной дисциплине	Решение, принятое кафедрой, разработавшей учебную программу
«Программно-аппаратные средства обеспечения информационной безопасности»	кафедра телекоммуникаций и информационных технологий	нет	изменений не требуется протокол № 3 от 16.10.2018

ДОПОЛНЕНИЯ И ИЗМЕНЕНИЯ К УЧЕБНОЙ ПРОГРАММЕ УВО
на _____ / _____ учебный год

№ п/п	Дополнения и изменения	Основание

Учебная программа пересмотрена и одобрена на заседании кафедры
_____ (протокол № _____ от _____ 20__ г.)

Заведующий кафедрой

(ученая степень, звание)

(подпись)

(И.О.Фамилия)

УТВЕРЖДАЮ
Декан факультета

(ученая степень, звание)

(подпись)

(И.О. Фамилия)