Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Максимов Алексей Борисович
Должность: директор департамента по образовательной политике
Дата подписания: 23.10.2023 16:38:18
Уникальный программный ключ:
8db180d1a3f02ac9e60521a5672742735c18b1d6

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»
(МОСКОВСКИЙ ПОЛИТЕХ)

Факультет информационных технологий

УТВЕРЖДАЮ
Декан факультета
информационных технологий
/Д. Г. Демидов/
"28" апреля 2022 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
«Защита встраиваемых систем и интернета вещей»

Направление подготовки 10.05.03
«Информационная безопасность автоматизированных систем»

Образовательная программа (профиль):
«Безопасность открытых информационных систем»

Квалификация (степень) выпускника
Специалист по защите информации

Год приема – 2022

Формы обучения
Очная

Москва, 2022 г.

Разработчик(и):

Доцент, к.т.н., доцент  /И.В. Калуцкий/

Согласовано:

И.о. заведующего кафедрой «Информационная безопасность»,  А.Ю. Гневшев

Руководитель образовательной программы,  А.Ю. Гневшев

Содержание

1	Цели, задачи и планируемые результаты обучения по дисциплине	4
2	Место дисциплины в структуре образовательной программы	5
3	Структура и содержание дисциплины	5
3.1	Виды учебной работы и трудоемкость	5
3.2	Тематический план изучения дисциплины	6
3.3	Содержание дисциплины	7
3.4	Тематика семинарских/практических и лабораторных занятий	8
3.5	Тематика курсовых проектов (курсовых работ)	9
4	Учебно-методическое и информационное обеспечение	9
4.1	Нормативные документы и ГОСТы	9
4.2	Основная литература	10
4.3	Дополнительная литература	10
4.4	Электронные образовательные ресурсы	11
4.5	Лицензионное и свободно распространяемое программное обеспечение	11
4.6	Современные профессиональные базы данных и информационные справочные системы	11
5	Материально-техническое обеспечение	11
6	Методические рекомендации	11
6.1	Методические рекомендации для преподавателя по организации обучения	11
6.2	Методические указания для обучающихся по освоению дисциплины	11
7	Фонд оценочных средств	11
7.1	Методы контроля и оценивания результатов обучения	11
7.2	Шкала и критерии оценивания результатов обучения	12
7.3	Оценочные средства	13

1 Цели, задачи и планируемые результаты обучения по дисциплине

Целями освоения дисциплины «Безопасность интернета вещей» являются:

- ознакомление студентов с основными принципами организации, функционирования и методами построения и защиты аппаратурно-программных средств, образующих компьютерные комплексы и системы, функционирующие в среде интернета вещей.
- ввести в круг понятий и задач в области Интернета Вещей, включая аппаратное, программное и сетевое обеспечение для того, чтобы студенты могли самостоятельно обнаруживать и формулировать существующие проблемы безопасности и предлагать обоснованные решения на основе IoT-технологий.

Задачи преподавания дисциплины:

- анализ состояния и тенденций развития вычислительной техники в т.ч., и существующих IoT-технологий и применение их на практике;
- изучение характеристик и режимов безопасной работы основных функциональных узлов и устройств вычислительных систем и комплексов, функционирующих в среде интернета вещей.
- формирование у студентов понимания важности развития и применения компьютерных комплексов и систем в современных технологиях как объективной закономерности развития информационного общества.

В результате освоения дисциплины «Защита встраиваемых систем и интернета вещей» у обучающихся формируются следующие компетенции и должны быть достигнуты следующие результаты обучения как этап формирования соответствующих компетенций:

- способен разрабатывать и эксплуатировать системы защиты информации открытых информационных систем

- способен осуществлять контроль обеспечения информационной безопасности и проводить верификацию данных в открытых информационных системах..

Обучение по дисциплине «Защита встраиваемых систем и интернета вещей» направлено на формирование у обучающихся следующих компетенций:

Код и наименование компетенций	Индикаторы достижения компетенции
ОПК-5.2. способен разрабатывать и эксплуатировать системы защиты информации открытых информационных систем	ИОПК-5.2.1 Выполняет обследование объекта защиты, обосновывает необходимость создания системы защиты информации, разрабатывает техническое задание на создание подсистемы информационной безопасности для открытой информационной системы; ИОПК-5.2.2 На основе требований к открытой информационной системе (технического, программного, информационного обеспечения и технологии обработки (передачи) информации) разрабатывает организационно-технические мероприятия по защите информации организационно-распорядительные документы по обеспечению информационной безопасности; ИОПК-5.2.3 Проводит опытную эксплуатацию средств защиты

	информации в комплексе с другими техническими и программными средствами открытой информационной системы, разрабатывает методики и документы приемо-сдаточных испытаний средств защиты информации
ОПК-5.3. способен осуществлять контроль обеспечения информационной безопасности и проводить верификацию данных в открытых информационных системах.	ОПК-5.3.1 Понимает значение контроля информационной безопасности, применяет различные виды контроля обеспечения информационной безопасности; ОПК-5.3.2 Проводит контроль эффективности защиты информации (организационный и технический) в открытых информационных системах ОПК-5.3.3 Определяет виды и категории данных, подлежащих обработке в открытой информационной системе, их объемы, структуру, технологии обработки и передачи, методы верификации и контроля целостности; проводит верификацию и контроль целостности данных

2 Место дисциплины в структуре образовательной программы

Дисциплина «Защита встраиваемых систем и интернета вещей» относится к числу учебных дисциплин обязательной части (Б1.1) основной образовательной программы (Б1.51).

Изучение дисциплины опирается на знания, умения и навыки, приобретенные в предшествующих дисциплинах: «Основы информационной безопасности», «Сети и системы передачи информации», «Безопасность систем баз данных», «Электроника и самотехника».

3 Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 4 зачетные единицы, т.е. 144 часа (лабораторные занятия – 72 час, самостоятельная работа - 72 часов, форма контроля – экзамен) в 7 семестре.

Структура и содержание дисциплины «Защита встраиваемых систем и интернета вещей» по срокам и видам работы отражены в приложении

3.1 Виды учебной работы и трудоемкость

(по формам обучения)

3.1.1 Очная форма обучения

№ п/п	Вид учебной работы	Количество часов	Семестры	
			9	
1	**Аудиторные занятия**	**72**	72	
	В том числе:			

1.1	Лекции			
1.2	Семинарские/практические занятия			
1.3	Лабораторные занятия	72	72	
2	**Самостоятельная работа**	**72**	72	
	В том числе:			
2.1	…			
3	**Промежуточная аттестация**			
	Зачет/диф.зачет/экзамен		экзамен	
	Итого			

3.1.2 Очно-заочная форма обучения
Не предусмотрена

3.1.3 Заочная форма обучения
Не предусмотрена

3.2 Тематический план изучения дисциплины
(по формам обучения)

3.2.1 Очная форма обучения

№ п/п	**Разделы/темы дисциплины**	**Трудоемкость, час**					
		Всего	**Аудиторная работа**				**Самостоятельная работа**
			Лекции	Семинарские/ практические занятия	Лабораторные занятия	Практическая подготовка	
1	Раздел 1. Инновационные технологии и безопасность техносферы						
1.1	Тема 1. Введение. Техносфера и ее эволюция – тенденции и угрозы.	4					4
1.2	Тема 2. Альтернативные источники энергии	4					4
1.3	Тема 3. Робототехника и мехатроника. Аддитивные технологии. Биокибернетика. Нанотехнологии	16			8		8
2	Раздел 2. Операционные системы и мобильные устройства						
2.1	Тема 1. Классификация ОС. Факторы, оказывающие влияние на структуру ОС.	6			2		4
2.2	Тема 2. Защищенные отечественные ОС	16			8		8
2.3	Тема 3. Astra Linux Special Edition	28			16		12

2.4	Тема 4. Тенденции развития мобильных ОС, версии и разновидности встраиваемых ОС	8			4		4
2.5	Тема 5. Мобильные устройства	14			6		8
3	Раздел 3. Технологии интернета вещей и защита информации						
3.1	Тема 1. Интернет вещей и тенденции его развития	2					2
3.2	Тема 2. Умный дом. Интеллектуальные и энергосберегающие технологии и системы	6			4		2
3.3	Тема 3. Протоколы передачи данных. Видеоконференцсвязь	10			6		4
3.4	Особенности технологий Zigbee и LoraWAN	10			6		4
3.5	Радиочастотная идентификация, QR- и штрих коды	10			6		4
3.6	Защита информации в сетях передачи данных IoT	10			6		4
	Итого	**144**			**72**		**72**

3.2.2 Очно-заочная форма обучения
Не предусмотрена.

3.2.2 Заочная форма обучения
Не предусмотрена

3.3 Содержание дисциплины

№ п/п	Раздел (тема) дисциплины	Содержание
1	2	3
1	Раздел 1. Инновационные технологии и безопасность техносферы	
1.1	Тема 1. Введение. Техносфера и ее эволюция – тенденции и угрозы.	Основные понятия. Тенденции развития техносферы, направления, интенсивность внедрения новых технологических решений в повседневной жизни человека..
1.2	Тема 2. Альтернативные источники энергии	Альтернативные и возобновляемые источники энергии. Технологии построения энергоэффективных объектов.
1.3	Тема 3. Робототехника и мехатроника. Аддитивные технологии. Биокибернетика. Нанотехнологии	Робототехника и мехатроника. Аддитивные технологии. Биокибернетика. Нанотехнологии. Новые технологии, тренды и их вовлеченность в науку, жизнь и технологическую среду.

2	Раздел 2. Операционные системы и мобильные устройства	
2.1	Тема 1. Классификация ОС. Факторы, оказывающие влияние на структуру ОС.	Windows, Linux, MacOS – сравнение и особенности. Android, iOS, Windows Phone – сравнение и особенности.
2.2	Тема 2. Защищенные отечественные ОС	Обзор защищенных операционных систем семейства Linux Архитектура, назначение и области применения Операционной Системы Специального Назначения Astra Linux Special Edition.
2.3	Тема 3. Astra Linux Special Edition	1.Основные задачи администрирования ASTRA LINUX SE. 2. Администрирование учётных записей пользователей и групп. 3.Администрирование процессов. 4. Администрирование устройств. 5. Особенности настройки контроля целостности и аутентификации в ОССН. 6. Сетевое взаимодействие в ОССН.
2.4	Тема 4. Тенденции развития мобильных ОС, версии и разновидности встраиваемых ОС	1. Встраиваемые системы. 2. Операционные системы для встраиваемых систем. 3. Системы реального времени. Примеры.
2.5	Тема 5. Мобильные устройства	Особенности использования и разработки мобильных приложений.
3	Раздел 3. Технологии интернета вещей и защита информации	
3.1	Тема 1. Интернет вещей и тенденции его развития	История зарождения интернета вещей, основные термины и понятия, тенденции развития.
3.2	Тема 2. Умный дом. Интеллектуальные и энергосберегающие технологии и системы	Парадигма умного здания, особенности, возможности, примеры.
3.3	Тема 3. Протоколы передачи данных. Видеоконференцсвязь	Протоколы передачи данных для устройств интернета вещей. Общие проблемы помехозащищенности каналов передачи данных IoT. Проблемы безопасности IoT.
3.4	Тема 4. Особенности технологий Zigbee и LoraWAN	Zigbee и LoraWAN – принципы, особенности, вопросы реализации, построение сети и масштабирование.
3.5	Тема 5. Радиочастотная идентификация, QR- и штрих коды	Технологии идентификации устройств IoT по радиоканалу, используемые частоты. QR- и штрих коды – технологии применения в различных вариантах.
3.6	Тема 6. Защита информации в сетях передачи данных IoT	Принципы защиты сетей IoT. Проблемы обеспечения безопасности и варианты решения, практические примеры.

3.4 Тематика семинарских/практических и лабораторных занятий

3.4.1 Семинарские/практические занятия

Не предусмотрены учебным планом.

3.4.2 Лабораторные занятия

№	Наименование лабораторной работы	Объем, час.
1	Выполнение работы №1 «Изучение тенденций в робототехнике, мехатронике, биокибернетике, нанотехнологиях»	8
2	Выполнение работы №2 «Сравнительный анализ операционных систем различных платформ»	2
3	Выполнение работы №3 «Знакомство с защищенными отечественными ОС»	8
4	Выполнение работы №4 «Сравнение Astra Linux Common Edition и Special Edition. Базовые функции»	2
5	Выполнение работы №5 «Аудит безопасности в ОССН Astra Linux SE»	6
6	Выполнение работы №6 «Безопасность доменной структуры сети в ОССН Astra Linux SE»	8
7	Выполнение работы №7 «Сравнительный анализ мобильных ОС»	4
8	Выполнение работы №8 «Мобильные платформы и их безопасность»	6
9	Выполнение работы №9 «Применение энергосберегающих технологий в умных домах»	4
10	Выполнение работы №10 «Организация видеоконференцсвязи с использованием умных устройств»	6
11	Выполнение работы №11 «Сравнительный анализ технологий Zigbee и LoraWAN»	6
12	Выполнение работы №12 «Применение QR- и штрих кодов для аутентификации и подключения устройств IoT»	6
13	Выполнение работы №13 «Защита информации в сетях передачи данных IoT”	6
Итого		72

3.5 Тематика курсовых проектов (курсовых работ)

Курсовое проектирование по данной дисциплине учебным планом не запланировано.

4 Учебно-методическое и информационное обеспечение

4.1 Нормативные документы и ГОСТы

1. Программа составлена в соответствии с Федеральным государственным образовательным стандартом высшего образования по направлению подготовки бакалавров 10.05.03 «Информационная безопасность автоматизированных систем».

4.2 Основная литература

1. «Архитектура операционных систем мобильных устройств» (Архитектура операционных систем мобильных устройств : учебное пособие / И. В. Синицын, С. М. Трушин, Ю. А. Воронцов, Е. К. Михайлова. — Москва : РТУ МИРЭА, 2022. — 343 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/265724

2. Белоус, А. И. Основы кибербезопасности. Стандарты, концепции, методы и средства обеспечения : энциклопедия / А. И. Белоус, В. А. Солодуха. — Москва : Техносфера, 2021. — 482 с. — ISBN 978-5-94836-612-8. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/181222

3. «Принципы построения и функционирования аппаратно-программных средств телекоммуникационных систем: Часть 2: Сетевые операционные системы и принципы обеспечения информационной безопасности в сетях» (Макаренко, С. И. Принципы построения и функционирования аппаратно-программных средств телекоммуникационных систем : учебное пособие / С. И. Макаренко, А. А. Ковальский, С. А. Краснов. — Санкт-Петербург : , 2020 — Часть 2 : Сетевые операционные системы и принципы обеспечения информационной безопасности в сетях — 2020. — ISBN 978-5-6044429-8-2. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/329378

4. Паршин, К. А. Методы и средства проектирования информационных систем и технологий : учебно-методическое пособие / К. А. Паршин. — Екатеринбург : , 2018. — 129 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/121337 (дата обращения: 01.02.2022). — Режим доступа: для авториз. пользователей. — С. 1.

4.3 Дополнительная литература

1. «Цифровая экономика и реиндустриализация производства: В 2 ч. Ч. 1. Развитие цифровой экономики и технологии реиндустриализации» (Цифровая экономика и реиндустриализация производства : учебное пособие : в 2 частях / Ю. А. Антохина, А. Г. Варжапетян, Е. Г. Семенова, М. С. Смирнова. — Санкт-Петербург : ГУАП, 2019 — Часть 1 : Развитие цифровой экономики и технологии реиндустриализации — 2019. — ISBN 978-5-8088-1416-5. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/165246

2. Терехов, А. В. ИТ-инфраструктура организации : учебное пособие / А. В. Терехов, В. Н. Чернышов, И. П. Рак. — Тамбов : ТГТУ, 2017. — ISBN 978-5-8265-1844-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/319799 (дата обращения: 01.02.2022). — Режим доступа: для авториз. пользователей. — С. 85.

3. Архитектурные решения информационных систем : учебник для вузов / А. И. Водяхо, Л. С. Выговский, В. А. Дубенецкий, В. В. Цехановский. — 3-е изд., стер. — Санкт-Петербург : Лань, 2022. — ISBN 978-5-507-44710-7. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/254624 (дата обращения: 01.02.2022). — Режим доступа: для авториз. пользователей. — С. 104.

4.4 Электронные образовательные ресурсы

1. Документация Yandex Cloud [Электронный ресурс] — URL: https://cloud.yandex.ru/docs (дата обращения: 01.02.2022).

4.5 Лицензионное и свободно распространяемое программное обеспечение

1. Операционная система Microsoft Windows от 7 версии и выше; Microsoft Office или Open Office, браузер (Firefox/Google Chrome /Explorer).

1.

4.6 Современные профессиональные базы данных и информационные справочные системы

1. Документация Yandex Cloud [Электронный ресурс] — URL: https://cloud.yandex.ru/docs (дата обращения: 01.02.2022).

5 Материально-техническое обеспечение

Для проведения всех видов занятий необходимо презентационное оборудование (мультимедийный проектор, экран) – 1 комплект.

Для проведения лабораторных занятий необходимо наличие компьютерных классов оборудованных современной вычислительной техникой из расчета одно рабочее место на одного обучаемого.

6 Методические рекомендации

6.1 Методические рекомендации для преподавателя по организации обучения

1. При подготовке к занятиям следует предварительно проработать материал занятия, предусмотрев его подачу точно в отведенное для этого время занятия. Следует подготовить необходимые материалы – теоретические сведения, задачи и др. При проведении занятия следует контролировать подачу материала и решение заданий с учетом учебного времени, отведенного для занятия.

2. При проверке работ и отчетов следует учитывать не только правильность выполнения заданий, но и оптимальность выбранных методов решения, правильность выполнения всех его шагов.

6.2 Методические указания для обучающихся по освоению дисциплины

Изучение дисциплины осуществляется в строгом соответствии с целевой установкой в тесной взаимосвязи учебным планом. Основой теоретической и практической подготовки студентов являются лекции и лабораторные работы.

В процессе самостоятельной работы студенты закрепляют и углубляют знания, полученные во время аудиторных занятий, готовятся к экзамену, а также самостоятельно изучают отдельные темы учебной программы.

7 Фонд оценочных средств

7.1 Методы контроля и оценивания результатов обучения

В процессе обучения используются следующие оценочные формы самостоятельной работы студентов, оценочные средства текущего контроля успеваемости и промежуточных аттестаций:

- проведение лабораторных работ (практических занятий с использованием спецтехники) и их защита;
- самостоятельная подготовка и проведение презентаций по темам дисциплины;
- экзамен.

7.2 Шкала и критерии оценивания результатов обучения

Форма промежуточной аттестации: экзамен.

По итогам промежуточной аттестации по дисциплине (модулю) выставляется оценка «отлично», «хорошо», «удовлетворительно» или «неудовлетворительно».

Шкала оценивания	Описание
Отлично	Выполнены все виды учебной работы, предусмотренные учебным планом. Студент демонстрирует соответствие знаний, умений, навыков приведенным в таблицах показателей, оперирует приобретенными знаниями, умениями, навыками, применяет их в ситуациях повышенной сложности. При этом могут быть допущены незначительные ошибки, неточности, затруднения при аналитических операциях, переносе знаний и умений на новые, нестандартные ситуации.
Хорошо	Выполнены все виды учебной работы, предусмотренные учебным планом. Студент демонстрирует неполное, правильное соответствие знаний, умений, навыков приведенным в таблицах показателей, либо если при этом были допущены 2-3 несущественные ошибки.
Удовлетворительно	Выполнены все виды учебной работы, предусмотренные учебным планом. Студент демонстрирует соответствие знаний, в котором освещена основная, наиболее важная часть материала, но при этом допущена одна значительная ошибка или неточность.
Неудовлетворительно	Не выполнен один или более видов учебной работы, предусмотренных учебным планом. Студент демонстрирует неполное соответствие знаний, умений, навыков приведенным в таблицах показателей, допускаются значительные ошибки, проявляется отсутствие знаний, умений, навыков по ряду показателей, студент испытывает значительные затруднения при оперировании знаниями и умениями при их переносе на новые ситуации.

7.3 Оценочные средства

7.3.1 Текущий контроль
Оценочные средства для текущей аттестации
- Защита отчетов о выполнении лабораторных работ

7.3.2 Промежуточная аттестация

Оценочные средства для промежуточной аттестации
- Экзамен

Список вопросов для экзамена по дисциплине:

1. Техносфера и ее эволюция- основные понятия.
2. Альтернативные и возобновляемые источники энергии.
3. Технологии построения энергоэффективных объектов.
4. Новые технологии, тренды и их вовлеченность в науку, жизнь и технологическую среду.
5. Встраиваемые ОС – ключевые особенности.
6. Приведите примеры (действительные) встраиваемых ОС и соответствующих сфер их применения.
7. Приведите примеры (действительные) защищенных ОС и соответствующих сфер их применения.
8. Особенности Android.
9. Особенности iOS.
10. Особенности Windows Phone.
11. Проблемы обеспечения безопасности операционных систем.
12. Подходы к построению защищенных операционных систем.
13. Основные функции подсистемы защиты операционной системы.
14. Идентификация, аутентификация и авторизация субъектов доступа.
15. Разграничение доступа к объектам операционной системы.
16. Основные модели разграничения доступа.
17. Изолированная программная среда.
18. Избирательное разграничение доступа.
19. Полномочное разграничение доступа с контролем информационных потоков.
20. Аудит в ОС как средство обеспечения безопасности.
21. Защищенные операционные системы семейства Linux (примеры и особенности кратко).
22. ОССН Astra Linux Special Edition (назначение и история появления).
23. ОССН Astra Linux Special Edition (Архитектура).
24. Подсистема обеспечения безопасности ОССН Astra Linux Special Edition (ключевые особенности).
25. Области применения ОССН Astra Linux Special Edition.
26. Отличия ОССН Astra Linux Special Edition от родительского дистрибутива Linux.
27. Перечислите уровни доступа приложений при обработке информации конкретными оконными приложениями (субъект-сессиями) с GUI-интерфейсом в соответствии с цветовым кодированием.
28. Ключевые особенности модели управления (разграничения) доступом в ОССН Astra Linux Special Edition.
29. Типы пользовательских сессий и их характеристика в ОССН.
30. Основные задачи администрирования ASTRA LINUX SE.
31. Администрирование устройств в ОССН (основные особенности).

32. Подсистема безопасности PARSEC в ASTRA LINUX SE (назначение и основные функции)
33. Проблемы реализации мандатного управления доступом в операционных системах.
34. Реализация мандатного управления доступом в ОССН (ключевые особенности).
35. Администрирование мандатного управления доступом в ОССН (утилиты администрирования и их назначение)
36. Уровни конфиденциальности в ОССН ASTRA LINUX SE.
37. Контроль целостности в ОССН ASTRA LINUX SE (особенности).
38. Управление доступом к объектам графической подсистемы в ОССН ASTRA LINUX SE.
39. Особенности аутентификации в ОССН ASTRA LINUX SE.
40. Особенности аудита в ОССН ASTRA LINUX SE.
41. Доменная структура в ОССН ASTRA LINUX SE (общая схема развертывания).
42. Особенности настройки резервного контроллера домена в сетевой инфраструктуре на основе ОССН.
43. История зарождения интернета вещей.
44. Основные термины и понятия, тенденции развития интернета вещей.
45. Парадигма умного здания.
46. Протоколы передачи данных для устройств интернета вещей.
47. Общие проблемы помехозащищенности каналов передачи данных IoT.
48. Проблемы безопасности IoT.
49. Технологии идентификации устройств IoT по радиоканалу.
50. QR- и штрих коды – технологии применения в различных вариантах, примеры.
51. Принципы защиты сетей IoT.
52. Проблемы обеспечения безопасности и варианты решения, практические примеры.

Пример билета.

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»
(МОСКОВСКИЙ ПОЛИТЕХ)

Факультет информационных технологий
Кафедра: Информационная безопасность
Дисциплина: Защита встраиваемых систем и интернета вещей
Специалисты. Курс 5, семестр 9

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 1

1. Операционная система МСВС – основные особенности.
2. Технология Zigbee – ключевые особенности.
3. ОССН Astra Linux Special Edition (назначение и история появления).
4. Особенности настройки резервного контроллера домена в сетевой инфраструктуре на основе ОССН ASTRA LINUX SE.

Преподаватель _____ / Калуцкий И.В. /
