МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное автономное образовательное учреждение высшего образования
«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

УТВЕРЖДЕНО
Декан факультета
Информационных технологий
_____ / Д.Г. Демидов /
«16» ___02_____ 2023 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Разработка интеллектуальных систем управления беспилотного транспорта»

Направление подготовки
09.03.01 «Информатика и вычислительная техника»

Профиль подготовки
«Киберфизические системы»

Квалификация (степень) выпускника:
Бакалавр

Форма обучения
Очная

Москва 2023 г.

Рабочая программа составлена на основе ФГОС ВО и учебного плана Московского политехнического университета по направлению (специальности) 09.03.01 Информатики и вычислительная техника, по профилю подготовки Киберфизические системы

Составители рабочей программы:

доцент кафедры «СМАРТ технологии», к.ф.-м.н.		Т. Т. Идиатуллов
(должность, ученое звание, степень)	(подпись)	(Ф.И.О.)

доцент кафедры «СМАРТ технологии», к.т.н., доцент		Д. И. Давлетчин
(должность, ученое звание, степень)	(подпись)	(Ф.И.О.)

Рабочая программа утверждена на заседании кафедры

СМАРТ технологии
(наименование кафедры)

Заведующий кафедрой к.т.н., доцент		Е. В. Петрунина
	(подпись)	(Ф.И.О.)

СОГЛАСОВАНО:

Заведующий кафедрой «СМАРТ технологии», к.т.н., доцент		Е. В. Петрунина
	(подпись)	(Ф.И.О.)

Аннотация к рабочей программе дисциплины
«Кибербезопасность систем интернета вещей и робототехники»

Дисциплина «Кибербезопасность систем интернета вещей и робототехники» реализуется в рамках образовательной программы высшего образования – программы бакалавриата по направлению подготовки (специальности) 09.03.01 Информатики и вычислительная техника по профилю подготовки Киберфизические системы обучения на русском языке.

Место в образовательной программе: Дисциплина «Кибербезопасность систем интернета вещей и робототехники» развивает знания, умения и навыки, сформированные у обучающихся по результатам изучения следующих дисциплин: «Математическая логика и теория алгоритмов», «Теория вероятностей и математическая статистика».

Дисциплина «Кибербезопасность систем интернета вещей и робототехники» реализуется в 5 семестре в рамках части, формируемой участниками образовательных отношений, дисциплин (модулей) Блока 1 и является дисциплиной по выбору.

Дисциплина «Кибербезопасность систем интернета вещей и робототехники» направлена на формирование компетенций:

Способен разрабатывать компоненты системных программных продуктов, вчасти следующих индикаторов достижения компетенции:

ПК-3	Уметь применять знания в области разработки ПО в предметной области
Знать проблемы возникающие при интеграции систем информационной безопасности в комплексные информационные системы, методы первичного анализа объекта защиты, технические и эксплуатационные характеристики основных элементов системы информационной безопасности **Уметь** определить функциональные и архитектурные требования к разрабатываемой СЗИ. **Владеть** проблемами возникающими при интеграции систем информационной безопасности в комплексные информационные системы, методы первичного анализа объекта защиты, технические и эксплуатационные характеристики основных элементов системы информационной безопасности.	

Перечень основных разделов дисциплины:

При освоении дисциплины студенты выполняют следующие виды учебной работы: лекции, практические занятия, консультации, самостоятельная работа. В учебном процессе предусматривается использование активных и интерактивных форм проведения занятий. В том числе, предполагаются, что на практических (семинарских) занятиях, которые проходят в интерактивном режиме, студенты должны проявлять активность при обсуждении темы семинара.

Самостоятельная работа включает: подготовку к практическим занятиям по разделам дисциплины, подготовку презентаций докладов, написание эссе и итогового реферата, подготовку к экзамену.

Правила аттестации по дисциплине. Текущий контроль по дисциплине «Кибербезопасность систем интернета вещей и робототехники» на практических занятиях на основании оценки запортфолио (задания по разделам дисциплины).

Промежуточная аттестация по дисциплине «Кибербезопасность систем интернета вещей и робототехники» проводится по завершению периода ее освоения (семестра) в форме экзамена.

Оценка «зачтено» за портфолио является необходимым условием для прохождения промежуточной аттестации. Результаты промежуточной (итоговой по дисциплине) аттестации определяются оценками «отлично», «хорошо», «удовлетворительно», «неудовлетворительно». Оценки «отлично», «хорошо», «удовлетворительно» означают успешное прохождение промежуточной аттестации.

Аннотация к рабочей программе дисциплины
«Кибербезопасность систем интернета вещей и робототехники»

Дисциплина «Кибербезопасность систем интернета вещей и робототехники» реализуется в рамках образовательной программы высшего образования – программы бакалавриата 09.03.01 ИНФОРМАТИКА И ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА, направленность (профиль): ПРОГРАММНАЯ ИНЖЕНЕРИЯ И КОМПЬЮТЕРНЫЕ НАУКИ по очной форме
обучения на русском языке.

Место в образовательной программе: Дисциплина «Кибербезопасность систем интернета вещей и робототехники» развивает знания, умения и навыки, сформированные у обучающихся по результатам изучения следующих дисциплин: «Математическая логика и теория алгоритмов», «Теория вероятностей и математическая статистика».

Дисциплина «Кибербезопасность систем интернета вещей и робототехники» реализуется в 7 семестре в рамках части, формируемой участниками образовательных отношений, дисциплин (модулей) Блока 1 и является дисциплиной по выбору.

Дисциплина «Кибербезопасность систем интернета вещей и робототехники» направлена на формированиекомпетенций:

Способен разрабатывать компоненты системных программных продуктов (ПКС-2), в части следующих индикаторов достижения компетенции:

ПКС-2.3 Уметь применять знания в области разаботки ПО в предметной области

Перечень основных разделов дисциплины:

При освоении дисциплины студенты выполняют следующие виды учебной работы: лекции, практические занятия, консультации, самостоятельная работа. В учебном процессе предусматривается использование активных и интерактивных форм проведения занятий. В том числе, предполагаются, что на практических (семинарских) занятиях, которые проходят в интерактивном режиме, студенты должны проявлять активность при обсуждении темы семинара.

Самостоятельная работа включает: подготовку к практическим занятиям по разделам дисциплины, подготовку презентаций докладов, написание эссе и итогового реферата, подготовку к экзамену.

Общий объем дисциплины – 2 зачетных единиц (72 часа).

№ п.п.	Вид учебной работы	Всего часов (академических)
		3 курс, 6 семестр
1	**Контактная работа обучающихся с преподавателем всего:**	36
1.1.	**Аудиторные работа (всего)**	36

	В том числе:	-
	Занятия лекционного типа (ЗЛТ)	18
	Занятия семинарского типа (ЗСТ) в т.ч.:	
	Практические, семинарские занятия (ПЗ/СЗ)	
	Лабораторные занятия (ЛЗ)	18
1.2	**Внеаудиторная работа обучающихся с преподавателем в электроннойинформационно-образовательной среде**	
2	**Самостоятельная работа**	36
	В том числе:	
2.1.	Изучение теоретического материала	
2.2.	Написание курсового проекта (работы)	
2.3.	Написание контрольной работы	
2.4.	Другие виды самостоятельной работы (реферат)	
3	**Промежуточная аттестация в форме контактной работы (зачет)**	
	Общая трудоемкость (час (акад.)/ зач. ед.)	**72/2**

Правила аттестации по дисциплине. Текущий контроль по дисциплине «Кибербезопасность систем интернета вещей и робототехники» на практических занятиях на основании оценки запортфолио (задания по разделам дисциплины).

Промежуточная аттестация по дисциплине «Кибербезопасность систем интернета вещей и робототехники» проводится по завершению периода ее освоения (семестра) в форме экзамена.

Оценка «зачтено» за портфолио является необходимым условием для прохождения промежуточной аттестации. Результаты промежуточной (итоговой по дисциплине) аттестации определяются оценками «отлично», «хорошо», «удовлетворительно», «неудовлетворительно». Оценки «отлично», «хорошо», «удовлетворительно» означают успешное прохождение промежуточной аттестации.

1. Требования к результатам освоения дисциплины

Таблица 2.1

Результаты изучения дисциплины по уровням освоения (иметь представление, знать, уметь, владеть)	**Формы организации занятий**		
	Лекции	**Практики / семинары**	**Самостоятельная работа**
ПК-3 Уметь применять знания в области разаботки ПО в предметной области			
1. Знать проблемы возникающие при интеграции систем информационной безопасности в комплексные информационные системы на базе систем и устройств Интернета вещей, методы разработки комплексных программных решений в защищенном исполнении, знать методики разработки безопасного прикладного программного обеспечения.	+	+	+
2. Уметь определить функциональные и архитектурные требования к разрабатываемой СЗИ, формировать модель нарушителя.	+	+	+

2. Содержание и структура учебной дисциплины

Таблица 3.1

Семестр: 5

	Темы лекций	Часы
1	Введение в проблему информационной безопасностиИнтернета вещей, области применения, специфика требований.	2
2	Жизненный цикл проекта Интернета вещей.	2
3	Классификация систем Интернета вещей. Нормативно-правовое регулирование. Требования к обеспечению информационной безопасности.	2
4	Обзор существующих методов защиты систем промышленных предприятия, требования и особенности интеграции элементов и систем защиты информации.	2
5	Управление рисками в системах интернета вещей. Классификация рисков, построение модели угроз. Критерии достаточности в управлении рисками Управление рисками как услуга: критерии качества.	2
6	Понятие модели нарушителя, отраслевые моделинарушителя	2

7	Влияние модели нарушителя на процесс разработки прикладного программного обеспечения.	2
8	Особенности применения криптографических средств при разработке компонент и модулей систем Интернета вещей.	2
	Итого:	**18**

Таблица 3.2

Темы практических занятий	**Часы**	**Учебная деятельность**
Введение в проблему информационной безопасности Интернета вещей, области применения,специфика требований.	2	Обучающиеся знакомятся с проблемой обеспечения безопасности элементов (датчиков, исполнительных устройств, элементов логикии автоматического принятиярешений). Выделяются основные отличительные черты систем от традиционных офисных систем и систем управления технологическими процессами.
Жизненный цикл проекта Интернета вещей	2	Рассматриваются основные этапы проекта создания комплексных систем на базестека технологий Интернетавещей, рассматриваются основные характеристики и потребности в безопасности.
Классификация систем Интернета вещей. Нормативно-правовое регулирование. Требования к обеспечению информационной безопасности.	2	Рассматриваются классы систем интернета вещей иформируется набор требований со стороны основных регуляторов к обеспечению информационной безопасности разрабатываемой системы.
Обзор существующих методов защиты систем промышленных предприятия,требования и особенности интеграции элементов и систем защиты информации.	2	Рассматриваются существующие методы и решения по защите информации, выявляются ихсильные и слабые стороны.
Управление рисками в	2	Обучающиеся знакомятся с

системах интернета вещей.Классификация рисков, построение модели угроз. Критерии достаточности в управлении рисками Управление рисками как услуга: критерии качества		принципами управления рисками, взаимосвязи моделей угроз и нарушителяс учетом выявленных рисков.
Понятие модели нарушителя,отраслевые модели нарушителя Влияние модели нарушителяна процесс разработки прикладного программного обеспечения	4	Обучающиеся проводят анализ выявленных рисков ина основе выполненного анализа разрабатывают краткую модель нарушителяс учетом требований контролирующих органов.
Методы снижения полной стоимости системы защиты информации.	4	Обучающиеся проводят анализ компонентной базы системы защиты информации, полученной на основе модели угроз и нарушителя и изучают методы снижения стоимости с учетом сложившихся бизнес-процессов и использованием компенсирующих мер в соответствии с требованиями регуляторов РФ.
Итого:	**18**	

3. Самостоятельная работа студентов

Таблица 4.1

№	Виды самостоятельной работы
Семестр: 6	
1	Обучающиеся повторяют теоретический материал, представленный на лекционном занятии, самостоятельно изучают рекомендованную основную и дополнительную литературу по соответствующим разделам дисциплины
2	По каждому разделу обучающиеся выполняют задание, входящее в портфолио. Результаты работы оформляются в виде эссе. Методические рекомендации по подготовке эссе представляются на лекции.
3	Подготовка к экзамену по вопросам, представленным в фонде оценочных средств, являющихся приложением к рабочей программе дисциплины.

4. Образовательные технологии

В ходе реализации учебного процесса по дисциплине проводятся лекционные и практические занятия. Темы, рассматриваемые на лекциях и изучаемые самостоятельно, закрепляются на практических занятиях, по вопросам, вызывающим затруднения, проводятся консультации на практических занятиях. Применяются такие формы проведения практических занятий, как обсуждение и защита результатов работы, а также используются интерактивные формы обучения.

Для организации и контроля самостоятельной работы студентов, а также проведения консультаций применяются информационно-коммуникационные технологии https://lms.mospolytech.ru

5. Правила аттестации студентов по учебной дисциплине

По дисциплине « Кибербезопасность систем интернета вещей и робототехники » проводится текущая и промежуточная аттестация (итоговая по дисциплине).

«Кибербезопасность систем интернета вещей и робототехники» на практических занятиях на основанииоценки за портфолио (написание и защита эссе по разделам дисциплины).

Требование к составу портфолио

1. По каждой из тем 1-6 необходимо подготовить задание, ответ оформить вписьменном виде в формате эссе, сдать не позднее указанного срока (не более 2х недель).

Для получения оценки «зачтено» эссе на каждую тему, соответствующую разделам дисциплины должно быть выполнено и отправлено в сроки изучения темы.

Примеры заданий по темам:

1. Ознакомиться с основными типами систем интернета вещей, в ходе самостоятельной работы выделить ключевые требования минимум для двух типов систем по своему выбору. К таким типам относятся системы технологического управления в концепции Умный дом, системы управления агрегатами и режимами работы автомобиля и д.р.
2. Изучить требования, рекомендации по разработке элементов инфраструктуры Интернета вещей, выделить базовые требования по обеспечению безопасности. Предложить варианты решения.
3. Провести анализ типовых решений для Интернета вещей, определить основные риски.
4. Провести сравнительный анализ решений по защите систем Интернета вещей от различных производителей: Cisco Systems, Infoteks, Positive Technology и др.
5. Провести сравнительный анализ в требованиях по информационной безопасности систем Интернета вещей в зависимости от профиля их использования.
6. Провести анализ методов безопасной разработки программного обеспечения для систем Интернета вещей, определить основные типы бизнес-процессов безопасной разработки.

Защита эссе:

Студент должен рассказать о проделанной работе, пояснить все этапы работы и обосновать решения.

Промежуточная аттестация по дисциплине «Кибербезопасность систем интернета вещей

и робототехники»проводится по завершению периода ее освоения (семестра) в форме экзамена.

Оценка «зачтено» за портфолио является необходимым условием для прохождения промежуточной аттестации. Результаты промежуточной (итоговой по дисциплине) аттестации определяются оценками «отлично», «хорошо», «удовлетворительно», «неудовлетворительно». Оценки «отлично», «хорошо», «удовлетворительно» означают успешное прохождение промежуточной аттестации.

7. Учебно-методическое и информационное обеспечение дисциплины

7.1 Нормативные документы и ГОСТы

1. Федеральный государственный образовательный стандарт высшего образования. Уровень высшего образования. Бакалавриат. Направление подготовки 09.03.01 "Информатика и вычислительная техника" (утв. приказом Министерства образования и науки РФ от 12 января 2016 г. N 5)
2. Приказ Министерства труда и социальной защиты Российской Федерации от 18 ноября 2013 г. № 679н «Об утверждении профессионального стандарта «Программист».

7.2. Основная литература:

1. Прохорова, О.В. Информационная безопасность и защита информации : учебник / О.В. Прохорова ; Министерство образования и науки РФ, Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Самарский государственный архитектурно-строительный университет». - Самара : Самарский государственный архитектурно-строительный университет, 2014. - 113 с. : табл., схем., ил. - Библиогр. в кн. - ISBN 978-5-9585-0603-3 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=438331
2. Загинайлов, Ю.Н. Теория информационной безопасности и методология защиты информации : учебное пособие / Ю.Н. Загинайлов. - Москва ; Берлин : Директ-Медиа, 2015. - 253 с. : ил. - Библиогр. в кн. - ISBN 978-5-4475-3946-7 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=276557
3. Учебно-методический комплекс по дисциплине «Инженерное проектирование систем информационной безопасности»: Пермяков, Р. А. Инженерное проектирование систем информационной безопасности: учебно-методическое пособие / Р. А. Пермяков. – Новосибирск: Изд-во Новосиб. гос. ун-та, 2009,.120 с. https://drive.google.com/file/d/1D3Vqwg3sL5j9lWuskCE2ooXJQjLph_40/view?usp=shar ing

7.3. Дополнительная литература

1. Пермяков, Р. А. Инженерное проектирование систем информационной безопасности [Электронный ресурс]: электронный учебно-методический комплекс / Р.А Пермяков ; Новосиб. гос. ун-т. - Новосибирск, [2012]. - Режим доступа: https://drive.google.com/file/d/1D3Vqwg3sL5j9lWuskCE2ooXJQjLph_40/view?usp=sharing- Загл. с экрана.

7.4 Электронные образовательные ресурсы

1. https://e.lanbook.com/ Электронно-библиотечная система издательства «Лань» (дата обращения 10.08.2023)
2. https://academia-moscow.ru/e_learning/pum/ Программно-учебные модули «Издательский центр «Академия». (дата обращения 10.08.2023)
3. ЭОР в разработке

7.5. Программное обеспечение

Для обеспечения реализации дисциплины используется стандартный комплект программного обеспечения (ПО), включающий регулярно обновляемое лицензионное ПО Windows и MS Office. Специализированное программное обеспечение не требуется. Профессиональные базы данных и информационные справочные системы

7.6. Интернет ресурсы

1. Полнотекстовые журналы Springer Journals за 1997-2015 г., электронные книги (2005-2016 гг.), коллекция научных биомедицинских и биологических протоколов SpringerProtocols, коллекция научных материалов в области физических наук и инжиниринга SpringerMaterials, реферативная БД по чистой и прикладной математике zbMATH.
2. Электронная библиотека диссертаций Российской государственной библиотеки (ЭБД РГБ)
3. БД Scopus (Elsevier)
4. Лицензионные материалы на сайте eLibrary.ru
5. Правовая БД «Консультант Плюс»
6. Правовая БД «Гарант»
7. Банка данных угроз безопасности информации ФСТЭК России

№ п/п	Наименование Интернет-ресурса	Краткое описание
1	Журнал «Вестник НГУ. Серия: Информацион-ные технологии» [Электронный ресурс]. – Режим доступа: https://journals.nsu.ru/jit/ . – Загл. с экрана	Полнотекстовые электронные копии статей в области вычислительный методов (с 2006 года).
2	Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. ФСТЭК России, 2008 г.[Электронный ресурс]. – Режим доступа: https://fstec.ru/component/attachments/download/290 – Документ	Методический документ ФСТЭК РФ
3	Cisco Systems, Inc. Online Privacy Statement [Электронный ресурс]. – Режим доступа: http://www.cisco.com/web/siteassets/legal/global/privacy_statement_ru.html. – Документ	Публичная политика безопасности вРФ компании Cisco
4	СТО БР ИББС- 1.4-2018. Стандарт банка России.Jобеспечение информационной безопасности организаций банковской системы Российской Федерации. Управление риском нарушения информационной безопасности при аутсорсинге. [Электронный ресурс]. – Режим доступа: http://www.cbr.ru/Content/Document/File/46919/s	Стандарт банка России определяющий методы управления риском нарушения информационнойбезопасности при аутсорсинге

	t-14-18.pdf - Документ	
5	СТО БР БФБО-1.5-2018. Стандарт банка России. Безопасность финансовых (банковских) операций. Управление инцидентами информационной безопасности. [Электронный ресурс]. – Режим доступа: http://www.cbr.ru/Content/Document/File/51269/st-15-18.pdf - Документ	Стандарт банка России определяющий методы управленияинцидентами информационной безопасности
6	СТО БР ИББС-1.0-2014. Стандарт банка России. Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения. [Электронный ресурс]. – Режим доступа : http://www.cbr.ru/Content/Document/File/46921/st-10-14.pdf - Документ	Стандарт банка России определяющий общие положения защиты информации в организацияхбанковской сферы
7	СТО БР ИББС-1.2-2014. Стандарт банка России. Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки соответствия информационной безопасности организаций банковской системы российской федерации требованиям СТО БР ИББС-1.0-2014. [Электронный ресурс]. – Режим доступа: http://www.cbr.ru/Content/Document/File/46922/st-12-14.pdf - Документ	Стандарт банка России определяющий методики оценки соответствия информационной безопасности организаций банковскойсферы.
8	Стандарт банка России. Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Аудит информационной безопасности. [Электронный ресурс]. – Режим доступа: http://www.cbr.ru/Content/Document/File/46923/st11.pdf - Документ	Стандарт банка России определяющий методики аудитаинформационной безопасности

8. Материально-техническое обеспечение

Таблица 10.1

№	Наименование	Назначение

1	Презентационное оборудование (мультимедиа-проектор, экран, компьютер для управления)	Для проведения лекционных и практических занятий
2	Компьютерный класс (с выходом в Internet)	Для организации самостоятельной работы обучающихся

Материально-техническое обеспечение образовательного процесса по дисциплине для обучающихся из числа лиц с ограниченными возможностями здоровья осуществляется согласно «Порядку организации и осуществления образовательной деятельности по образовательным программам для инвалидов и лиц с ограниченными возможностями здоровья в Новосибирском государственном университете».

Приложение1
Перечень вопросов зачета

Вопрос 1. Причины уязвимости систем класса интерне-та вещей.
Вопрос 2. Интернет вещей, - основные виды уязвимостей компонентов
Вопрос 3. Требования к безопасности информационным
системам, основные нормативно-правовые акты.
Вопрос 4. Требования к безопасности информационнымсистемам, нормативно-правовые акты в области криптографической защиты.
Вопрос 5. Являются ли системы интернета вещей ключевыми? Приведение обоснование.
Вопрос 6. Жизненный цикл проекта Интернета вещей,характеристика этапов с точки зрения информационной
безопасно.
Вопрос 7. Влияние принципов SDLC на проект Интернета вещей.
Вопрос 8. Понятие информационной безопасности в системах интернета вещей.
Вопрос 9. Определение приоритетной задачи безопасности для систем интернета вещей.
Вопрос 10. Типовые архитектуры безопасности для интернета вещей.
Вопрос 11. Основные методы управления рисками.
Вопрос 12. Особенности модели угроз для интернета
вещей.
Вопрос 13. Назначение модели угроз.
Вопрос 14. Основные принципы управления рисками..
Вопрос 15. Роль модели угроз при разработке программного обеспечения.
Вопрос 16. Понятие безопасной разработки программного обеспечения.
Вопрос 17. Роль модели нарушителя при разработке
программного обеспечения
Вопрос 18. Состав раздела пользовательской документации по требованиям безопасности.
Вопрос 19. Включение элементов интернета вещей вкомплексные информационные системы, формирование
требований по безопасности.
Вопрос 20. Особенности интеграции сторонних решений в критическое программное обеспечение.
Вопрос 21. Роль модели нарушителя при разработке
безопасного программного обеспечения.
Вопрос 22. Включение элементов интернета вещей в
комплексные информационные системы,.
Вопрос 23. Влияние модели нарушителя компонента на
политику безопасности комплексной системы.
Вопрос 24. Понятие технических условий безопасного
использование компонентов.
Вопрос 25. Источники информации для построения модели нарушителя.
Вопрос 26. Роль эксперта в процессе разработки модели
нарушителя.
Вопрос 27. Управление рисками в системах интернета
вещей.
Вопрос 28. Классификация рисков для систем интернета
вещей.

Вопрос 29. Методики построения модели угроз.
Вопрос 30. Критерии достаточности в управлении рисками.
Вопрос 31. Управление рисками в системах интернета вещей как услуга: критерии качества.
Вопрос 32. Влияние модели нарушителя на процесс разработки прикладного программного обеспечения.
Вопрос 33. 11. Критерии достаточности при анализе безопасности прикладного программного обеспечения.
Вопрос 34. Понятие безопасной разработки программного обеспечения.
Вопрос 35. Состав типовой СЗИ для интернета вещей.
Вопрос 36. Методы управления процессами обмена информацией в системах интернета вещей.