Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования «Новосибирский национальный исследовательский
государственный университет» (Новосибирский государственный университет, НГУ)

Факультет информационных технологий

СОГЛАСОВАНО
Декан ФИТ НГУ
М.М. Лаврентьев
«03» июля 2019 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Безопасность в IoT (Интернет вещей)

Направление подготовки: 09.03.01 ИНФОРМАТИКА И ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА
Направленность (профиль): Программная инженерия и компьютерные науки

Форма обучения: очная
Год обучения: 4, семестр: 7

№	Вид деятельности	Семестр
		7
1	Лекции, час.	32
2	Практические занятия, час.	32
3	Лабораторные занятия, час.	
4	Занятий в контактной форме без учета промежуточной аттестации, час, из них	66
5	в электронной форме, час.	
6	из них аудиторных занятий, час.	64
7	из них в активной и интерактивной форме, час.	64
8	консультаций, час.	2
9	Самостоятельная работа, час.	76
10	в том числе на выполнение письменных работ, час	30
11	Форма аттестации (экзамен, зачет, дифференцированный зачет), час	Э 2
12	Всего зачетных единиц[1]	4

Новосибирск 2019

[1] С учетом выделенных часов на промежуточную аттестацию

Рабочая программа дисциплины составлена на основании федерального государственного образовательного стандарта (ФГОС) высшего образования - бакалавриат по направлению подготовки 09.03.01 ИНФОРМАТИКА И ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА.

Федеральный государственный образовательный стандарт (ФГОС) высшего образования - бакалавриат по направлению подготовки 09.03.01 ИНФОРМАТИКА И ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА введен в действие приказом Минобрнауки от 19.09.2017 № 929.

Место дисциплины в структуре учебного плана: Блок 1 Дисциплины (модули); часть, формируемая участниками образовательных отношений, дисциплина по выбору

Рабочая программа дисциплины утверждена решением Ученого совета факультета информационных технологий от 02.07.2019, протокол № 75.

Программу разработал:

старший преподаватель кафедры систем информатики ФИТ Р.А. Пермяков

Заведующий кафедрой систем информатики ФИТ,
доктор физико-математических наук М.М. Лаврентьев

Ответственный за образовательную программу:

доцент кафедры систем информатики ФИТ,
кандидат технических наук А.А.Романенко

Аннотация к рабочей программе дисциплины
«Безопасность в IoT (Интернет вещей)»

Дисциплина «Безопасность в IoT (Интернет вещей)» 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 «Безопасность в IoT (Интернет вещей)» развивает знания, умения и навыки, сформированные у обучающихся по результатам изучения следующих дисциплин: «Математическая логика и теория алгоритмов», «Теория вероятностей и математическая статистика».

Дисциплина «Безопасность в IoT (Интернет вещей)» реализуется в 7 семестре в рамках части, формируемой участниками образовательных отношений, дисциплин (модулей) Блока 1 и является дисциплиной по выбору.

Дисциплина «Безопасность в IoT (Интернет вещей)» направлена на формирование компетенций:

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 – 4 зачетных единиц (144 часа).

Правила аттестации по дисциплине. Текущий контроль по дисциплине «Безопасность в IoT (Интернет вещей)» на практических занятиях на основании оценки за портфолио (задания по разделам дисциплины).

Промежуточная аттестация по дисциплине «Безопасность в IoT (Интернет вещей)» 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.

Учебно-методическое обеспечение дисциплины.

Учебно-методический комплекс по дисциплине «Безопасность в IoT (Интернет вещей)»: 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=sharing

1. Внешние требования к дисциплине

Таблица 1.1

Компетенция ПКС-2 Способен разрабатывать компоненты системных программных продуктов*, в части следующих индикаторов достижения компетенции:*
ПКС-2.3 Уметь применять знания в области разаботки ПО в предметной области

2. 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**
ПКС-2.3 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.	+	+	+

3. Содержание и структура учебной дисциплины

Таблица 3.1

Темы лекций	**Активные формы, час. (входит в общее кол-во часов)**	**Часы**	**Ссылки на результаты обучения**
Семестр: 7			
— Введение в проблему информационной безопасности Интернета вещей, области применения, специфика требований.	2	2	1, 2
— Жизненный цикл проекта Интернета вещей.	4	4	1, 2
— Классификация систем Интернета вещей. Нормативно-правовое регулирование. Требования к обеспечению информационной безопасности.	6	6	1, 2
— Обзор существующих методов защиты систем промышленных предприятия, требования и особенности интеграции элементов и систем защиты информации.	4	4	1, 2
— Управление рисками в системах интернета вещей. — Классификация рисков, построение модели угроз. — Критерии достаточности в управлении рисками — Управление рисками как услуга: критерии качества.	4	4	1, 2
— Понятие модели нарушителя, отраслевые модели нарушителя	6	6	1, 2

— Влияние модели нарушителя на процесс разработки прикладного программного обеспечения.			
— Особенности применения криптографических средств при разработке компонент и модулей систем Интернета вещей.	6	6	1, 2
Итого:	**32**	**32**	

Таблица 3.2

Темы практических занятий	**Активные формы, час. (входит в общее кол-во часов)**	**Часы**	**Ссылки на результаты обучения**	**Учебная деятельность**
Семестр: 7				
Введение в проблему информационной безопасности Интернета вещей, области применения, специфика требований.	2	2	1, 2	Обучающиеся знакомятся с проблемой обеспечения безопасности элементов (датчиков, исполнительных устройств, элементов логики и автоматического принятия решений). Выделяются основные отличительные черты систем от традиционных офисных систем и систем управления технологическими процессами.
Жизненный цикл проекта Интернета вещей	6	6	1, 2	Рассматриваются основные этапы проекта создания комплексных систем на базе стека технологий Интернета вещей, рассматриваются основные характеристики и потребности в безопасности.
Классификация систем Интернета вещей. Нормативно-правовое регулирование. Требования к обеспечению информационной безопасности.	4	4	1, 2	Рассматриваются классы систем интернета вещей и формируется 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.	4	4	1, 2	Рассматриваются существующие методы и решения по защите информации, выявляются их сильные и слабые стороны.
Управление рисками в	4	4	1, 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 нарушителя с учетом выявленных рисков.
Понятие модели нарушителя, отраслевые модели нарушителя Влияние модели нарушителя на процесс разработки прикладного программного обеспечения	6	6	1, 2	Обучающиеся проводят анализ выявленных рисков и на основе выполненного анализа разрабатывают краткую модель нарушителя с учетом требований контролирующих органов.
Методы снижения полной стоимости системы защиты информации.	6	6	1, 2	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:	**32**	**32**		

4. Самостоятельная работа студентов

Таблица 4.1

№	Виды самостоятельной работы	Ссылки на результаты обучения	Часы на выполнение	Часы на консультации
Семестр: 7				
1	Подготовка к практическим занятиям по разделам дисциплины	1, 2	22	0
	Обучающиеся повторяют теоретический материал, представленный на лекционном занятии, самостоятельно изучают рекомендованную основную и дополнительную литературу по соответствующим разделам дисциплины			
6	Выполнение заданий в рамках портфолио	1,2	30	0
	По каждому разделу обучающиеся выполняют задание, входящее в портфолио. Результаты работы оформляются в виде эссе. Методические рекомендации по подготовке эссе представляются на лекции. https://drive.google.com/file/d/1D3Vqwg3sL5j9lWuskCE2ooXJQjLph_40/view?usp=sharing			
7	Подготовка к экзамену	1, 2	24	2
	Подготовка к экзамену по вопросам, представленным в фонде оценочных средств, являющихся приложением к рабочей программе дисциплины.			
	Итого:		**76**	**2**

5. 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 следующие интерактивные формы обучения (таблица 5.1).

Таблица 5.1

1	Технологии проблемного обучения	ПКС-2.3
Формируемые умения: 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.		
Краткое описание применения: Постановка под руководством преподавателя проблемных задач и активная самостоятельная деятельность обучающихся по их разрешению, сопровождающаяся обсуждением и защитой результатов.		
2	Портфолио	ПКС-2.3
Формируемые умения: 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.		
Краткое описание применения: обучающиеся ведут портфолио, которое является основой для проведения аттестации по дисциплине.		

Для организации и контроля самостоятельной работы студентов, а также проведения консультаций применяются информационно-коммуникационные технологии (таблица 5.2).

Таблица 5.2

Информирование	http://my.nsu.ru/uisws/ для взаимодействия с группой и рассылки дополнительных материалов
Консультирование	pra@yandex.ru – для отсылки работ и вопросов преподавателю. http://my.nsu.ru/uisws/ для взаимодействия с группой и рассылки дополнительных материалов
Контроль	http://my.nsu.ru/uisws/ для взаимодействия с группой и индивидуальных вопросов студентов.
Размещение учебных материалов	https://drive.google.com/drive/folders/1AbtgEu13kdi45Sba3JPbLwqC4mYdH35l?usp=sharing

6. Правила аттестации студентов по учебной дисциплине

По дисциплине «Безопасность в IoT (Интернет вещей)» проводится текущая и промежуточная аттестация (итоговая по дисциплине).

«Безопасность в IoT (Интернет вещей)» на практических занятиях на основании оценки 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 в письменном 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 «Индустрия 4.0», 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 «Безопасность в IoT (Интернет вещей)» 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.

В таблице 6.1 представлено соответствие форм аттестации заявляемым требованиям к результатам освоения дисциплины.

Таблица 6.1

Коды компетенций ФГОС	**Результаты обучения**	**Формы аттестации**	
		портфолио	**Экзамен**
ПКС-2	ПКС-2.3 Уметь применять знания в области разработки ПО в предметной области	+	+

Требования к структуре и содержанию портфолио, оценочные средства, а также критерии оценки сформированности компетенций и освоения дисциплины в целом, представлены в Фонде оценочных средств, являющемся приложением 1 к настоящей рабочей программе дисциплины.

7. 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

Интернет-ресурсы

Таблица 7.1

№ п/п	Наименование Интернет-ресурса	Краткое описание
1	Журнал «Вестник НГУ. Серия: Информационные 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 в РФ 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/st-14-18.pdf - Документ	Стандарт банка России определяющий методы управления риском нарушения информационной безопасности при аутсорсинге

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 управления инцидентами 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 организациях банковской 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 банковской сферы.
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 аудита информационной безопасности

8. Учебно-методическое и программное обеспечение дисциплины

8.1. Учебно-методическое обеспечение

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.

8.2. 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.

9. Профессиональные базы данных и информационные справочные системы

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

10. 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».

Лист актуализации рабочей программы дисциплины
«Безопасность в IoT (Интернет вещей)»

№	Характеристика внесенных изменений (с указанием пунктов документа)	Дата и № протокола Ученого совета ФИТ	Подпись ответственного
1.	Актуализирована на 2020-2021 уч.год	22.07.2020 №77	

Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования «Новосибирский национальный исследовательский
государственный университет» (Новосибирский государственный университет, НГУ)

Факультет информационных технологий

СОГЛАСОВАНО
Декан ФИТ НГУ
М.М. Лаврентьев
«03» июля 2019 г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ
по дисциплине Безопасность в IoT (Интернет вещей)

Направление подготовки: 09.03.01 ИНФОРМАТИКА И ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА

Направленность (профиль): Программная инженерия и компьютерные науки

Квалификация: бакалавр

Форма обучения: очная Год обучения: 4, семестр 7

Форма аттестации	Семестр
Экзамен	7

Новосибирск 2019

Фонд оценочных средств промежуточной аттестации по дисциплине является **Приложением 1** к рабочей программе дисциплины «Безопасность в IoT (Интернет вещей)», реализуемой в рамках образовательной программы высшего образования – программы бакалавриата 09.03.01 Информатика и вычислительная техника, направленность (профиль): Программная инженерия и компьютерные науки

Фонд оценочных средств промежуточной аттестации по дисциплине утвержден решением ученого совета факультета информационных технологий, протокол № 75 от 02.07.2019.

Разработчики:
старший преподаватель
кафедры систем информатики ФИТ — Р.А. Пермяков

Заведующий кафедрой систем информатики ФИТ,
доктор физико-математических наук — М.М. Лаврентьев

Ответственный за образовательную программу:
доцент кафедры систем информатики ФИТ,
кандидат технических наук — А.А. Романенко

1. Содержание и порядок проведения промежуточной аттестации по дисциплине

1.1. Общая характеристика содержания промежуточной аттестации

Промежуточная (итоговая по дисциплине) аттестация по дисциплине «Безопасность в IoT (Интернет вещей)» проводится по завершению периода освоения образовательной программы (семестра) для оценки сформированности компетенций в части следующих индикаторов достижения компетенции (таблица П1.1).

Таблица П1.1

Код	Компетенции, формируемые в рамках дисциплины «Безопасность в IoT (Интернет вещей)»	Семестр 7	
		Портфолио	Экзамен
ПКС-2	**Способен разрабатывать компоненты системных программных продуктов**		
ПКС-2.3	Уметь применять знания в области разработки ПО в предметной области	+	+

Промежуточная аттестация по дисциплине включает 2 этапа: портфолио и экзамен.

Тематика экзаменационных вопросов включает следующие темы (разделы):

1. Интернет вещей, - основные виды уязвимостей компонентов.
2. Требования к безопасности информационным системам, основные нормативно-правовые акты.
3. Жизненный цикл проекта Интернета вещей, характеристика этапов с точки зрения информационной безопасности.
4. Понятие информационной безопасности в системах интернета вещей.
5. Назначение модели угроз, особенности модели угроз для интернета вещей.
6. Основные принципы управления рисками.
7. Включение элементов интернета вещей в комплексные информационные системы, формирование требований по безопасности.
8. Включение элементов интернета вещей в комплексные информационные системы, влияние модели нарушителя компонента на политику безопасности комплексной системы.
9. Управление рисками в системах интернета вещей.
10. Классификация рисков, построение модели угроз.
11. Критерии достаточности при анализе безопасности прикладного программного обеспечения.
12. Управление рисками как услуга: критерии качества

13. Влияние модели нарушителя на процесс разработки прикладного программного обеспечения.
14. Критерии достаточности в управлении рисками.
15. Понятие безопасной разработки программного обеспечения.

1.2. Порядок проведения промежуточной аттестации по дисциплине

Промежуточная аттестация проводится в форме экзамена и включает 2 этапа: портфолио и экзамен. Необходимым условием для прохождения промежуточной аттестации является оценка «зачтено» за портфолио. Оценка «зачтено» за портфолио выставляется при условии выполнения и защиты работы.

Экзамен проводится в устной форме, по билетам. Билет выбирается обучающимся случайным образом. При подготовке ответа на вопросы билета не разрешается использование каких-либо источников информации. В процессе ответа обучающегося на вопросы билета преподаватель может задавать дополнительные вопросы по темам дисциплины. Результаты промежуточной аттестации определяются оценками «отлично», «хорошо», «удовлетворительно», «неудовлетворительно». Оценки «отлично», «хорошо», «удовлетворительно» означают успешное прохождение промежуточной аттестации.

2. Требования к структуре и содержанию фонда оценочных средств промежуточной аттестации по дисциплине

Перечень оценочных средств, применяемых на каждом этапе проведения промежуточной аттестации по дисциплине, представлен в таблице П1.2.

Таблица П1.2

№ п/п	Наименование оценочного средства	Краткая характеристика оценочного средства	Представление оценочного средства в фонде
Этап 1 - портфолио			
1	Портфолио	Целевая подборка работ студента, раскрывающая его индивидуальные образовательные достижения в одной или нескольких учебных дисциплинах.	Структура портфолио
Этап 2 - экзамен			
2	Экзаменационный билет	Комплекс вопросов	Список теоретических вопросов

2.1 Требования к структуре и содержанию оценочных средств аттестации

2.1.1 Требования к структуре и содержанию портфолио

Требование к составу портфолио

По каждой из тем 1-6 необходимо подготовить задание, ответ оформить в письменном 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.

Каждый студент формулирует задачу в рамках изучаемой темы. Формулировка согласовывается с преподавателем, при необходимости, преподаватель корректирует/уточняет постановку задачи.

Требования к представлению результатов.

Результаты выполненных заданий оформляются в формате эссе. Эссе необходимо представить:

- формулировку проблемы;
- обзор действующих ограничений на выбор решения
- обоснование выбора методов решения;
- структурное описания выбранного решения.

Авторы лучших эссе приглашаются для выступления на семинарском занятии с докладом.

Длительность доклада не превышает 5 минут.

По результатам анализа эссе выставляется оценка «зачтено» или «не зачтено». Оценка «зачтено» является необходимым условием для прохождения промежуточной аттестации.

Примеры тем заданий, входящих в состав портфолио:

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 «Индустрия 4.0», 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.

2.1.2 Форма и перечень вопросов экзаменационного билета

Форма экзаменационного билета

Таблица П1.3

Новосибирский государственный университет
Экзамен

Безопасность в IoT (Интернет вещей)
наименование дисциплины

09.03.01 ИНФОРМАТИКА И ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА
Программная инженерия и компьютерные науки
наименование образовательной программы

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №

1. Вопрос из категории 1
2. Вопрос из категории 2

Составитель _____Р.А.Пермяков
(подпись)

Ответственный за образовательную программу

_____ А.А. Романенко
(подпись)

«____»_____20 г.

Перечень вопросов экзамена, структурированный по категориям, представлен в таблице П1.4

Таблица П1.4

Категория	Формулировка вопроса
Категория 1 (ПКС-2.3)	Вопрос 1. Причины уязвимости систем класса интернета 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 информационным системам, 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.
Категория 2 (ПКС-2.3)	Вопрос 19. Включение элементов интернета вещей в комплексные 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.

Набор экзаменационных билетов формируется и утверждается в установленном порядке в начале учебного года при наличии контингента обучающихся, завершающих освоение дисциплины «Безопасность в IoT (Интернет вещей)» в текущем учебном году.

3. Критерии оценки сформированности компетенций в рамках промежуточной аттестации по дисциплине

Таблица П1.5

Шифр компетенций	**Структурные элементы оценочных средств**	**Показатель сформированности**	**Не сформирован (2 балла)**	**Пороговый уровень (3 балла)**	**Базовый уровень (4 балла)**	**Продвинутый уровень (5 баллов)**
ПКС-2	Экзаменационный билет	ПКС-2.3 Уметь применять знания в области разработки ПО в предметной области	Не может обосновать потребность в обеспечении безопасности систем интернета вещей.	Демонстрирует фрагментарные знания методик создания безопасного Прикладного программного обеспечения для интернета вещей.	демонстрирует базовые знания предмета, знает особенности методов анализа требований регуляторов к СЗИ для систем интернета вещей.	демонстрирует углубленные знания предмета, методов анализа угроз и моделей нарушителя при создании СЗИ для систем интернета вещей.
ПКС-2	Портфолио	ПКС-2.3 Уметь применять знания в области разработки ПО в предметной области	Не умеет сформулировать предложения по структуре СЗИ для систем интернета вещей.	демонстрирует фрагментированные знания методов анализа требований к СЗИ	демонстрирует базовые знания предмета, знает особенности методов анализа требований регуляторов к СЗИ для систем интернета вещей.	демонстрирует углубленные знания предмета, методов анализа угроз и моделей нарушителя при создании СЗИ для систем интернета вещей.

4. Критерии выставления оценок по результатам промежуточной аттестации по дисциплине

Результаты промежуточной аттестации в семестре определяются оценками «отлично», «хорошо», «удовлетворительно», «неудовлетворительно». Оценки «отлично», «хорошо», «удовлетворительно» означают успешное прохождение промежуточной аттестации.

Решение об окончательной оценке принимается по результатам 2 этапа (экзамена).

Оценка «отлично» соответствует продвинутому уровню сформированности компетенции.

Оценка «хорошо» соответствует базовому уровню сформированности компетенции.

Оценка «удовлетворительно» соответствует пороговому уровню сформированности компетенции.

Оценка «неудовлетворительно» выставляется при неудовлетворительном прохождении одного или двух этапов промежуточной аттестации.

Лист актуализации фонда оценочных средств
промежуточной аттестации по дисциплине
«Безопасность в IoT (Интернет вещей)»

№	Характеристика внесенных изменений (с указанием пунктов документа)	Дата и № протокола Ученого совета ФИТ	Подпись ответственного
1.	Актуализирован на 2020-2021 уч.год	22.07.2020 №77