МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

БЕЗОПАСНОСТЬ ИНТЕРНЕТА ВЕЩЕЙ

Направление подготовки (специальность)
10.05.03 Информационная безопасность автоматизированных систем

Направленность (профиль/специализация) программы
10.05.03 специализация N 8 "Разработка автоматизированных систем в защищенном исполнении"

Уровень высшего образования - специалитет

Форма обучения
очная

Институт/	Институт энергетики и автоматизированных систем
Кафедра	Информатики и информационной безопасности
Курс	3
Семестр	6

Магнитогорск
2025 год

Рабочая программа составлена на основе ФГОС ВО - специалитет по специальности 10.05.03 Информационная безопасность автоматизированных систем

Лист актуализации рабочей программы

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2026 - 2027 учебном году на заседании кафедры Информатики и информационной безопасности

Протокол от __ _____ 20__ г. № __
Зав. кафедрой _____ И.И. Баранкова

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2027 - 2028 учебном году на заседании кафедры Информатики и информационной безопасности

Протокол от __ _____ 20__ г. № __
Зав. кафедрой _____ И.И. Баранкова

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2028 - 2029 учебном году на заседании кафедры Информатики и информационной безопасности

Протокол от __ _____ 20__ г. № __
Зав. кафедрой _____ И.И. Баранкова

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2029 - 2030 учебном году на заседании кафедры Информатики и информационной безопасности

Протокол от __ _____ 20__ г. № __
Зав. кафедрой _____ И.И. Баранкова

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2030 - 2031 учебном году на заседании кафедры Информатики и информационной безопасности

Протокол от __ _____ 20__ г. № __
Зав. кафедрой _____ И.И. Баранкова

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2031 - 2032 учебном году на заседании кафедры Информатики и информационной безопасности

Протокол от __ _____ 20__ г. № __
Зав. кафедрой _____ И.И. Баранкова

1 Цели освоения дисциплины (модуля)

Целью дисциплины «Безопасность Интернета вещей» является формирование профессиональных навыков проектирования безопасных IoT-систем в соответствии с требованиями ФГОС ВО по специальности «Информационная безопасность автоматизированных систем». Дисциплина «Безопасность Интернета вещей» рассматривает базовые теоретические понятия, принципы проектирования надежных систем на базе IoT-устройств, средства и способы обеспечения информационной безопасности в IoI-системах.

2 Место дисциплины (модуля) в структуре образовательной программы

Дисциплина Безопасность Интернета вещей входит в часть учебного плана, формируемую участниками образовательных отношений образовательной программы.

Для изучения дисциплины необходимы знания (умения, владения), сформированные в результате изучения дисциплин/ практик:

Безопасность сетей ЭВМ

Безопасность операционных систем

Технологии и методы программирования

Сети и системы передачи информации

Основы информационной безопасности

Основы Data инжиниринга

Основы безопасности цифрового общества

Организация ЭВМ и вычислительных систем

Электроника и схемотехника

Знания (умения, владения), полученные при изучении данной дисциплины будут необходимы для изучения дисциплин/практик:

Методы выявления нарушений информационной безопасности

Тестирование систем защиты информации автоматизированных систем

Анализ уязвимостей программного обеспечения

Анализ рисков информационной безопасности

Обеспечение информационной безопасности критической информационной инфраструктурой

3 Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля) и планируемые результаты обучения

В результате освоения дисциплины (модуля) «Безопасность Интернета вещей» обучающийся должен обладать следующими компетенциями:

Код	Индикатор достижения компетенции
ПК-6 Способен проводить анализ структурных и функциональных схем защищенных автоматизированных информационных систем с целью выявления потенциальных уязвимостей информационной безопасности автоматизированных систем	
ПК-6.1	Проводит анализ структурных и функциональных схем защищенных автоматизированных информационных систем с целью выявления потенциальных уязвимостей информационной безопасности автоматизированных систем
ПК-6.2	Выявляет уязвимости информационно-технологических ресурсов автоматизированных систем
ПК-6.3	Выявляет основные угрозы безопасности информации в автоматизированных системах
ПК-6.4	Составляет протоколы тестирования систем защиты информации автоматизированных систем

ПК-7 Способен разрабатывать проектные решения по защите информации в автоматизированных системах	
ПК-7.1	Разрабатывает модели угроз безопасности информации и модели нарушителя в автоматизированных системах
ПК-7.2	Выбирает меры защиты информации, подлежащие реализации в системе защиты информации автоматизированной системы
ПК-7.3	Определяет виды и типы средств защиты информации, обеспечивающих реализацию технических мер защиты информации
ПК-7.4	Определяет структуру системы защиты информации автоматизированной системы в соответствии с требованиями нормативных правовых документов в области защиты информации автоматизированных систем

4. Структура, объём и содержание дисциплины (модуля)

Общая трудоемкость дисциплины составляет 3 зачетных единиц 108 акад. часов, в том числе:

– контактная работа – 51,95 акад. часов:

– аудиторная – 51 акад. часов;

– внеаудиторная – 0,95 акад. часов;

– самостоятельная работа – 56,05 акад. часов;

– в форме практической подготовки – 0 акад. час;

Форма аттестации - зачет

Раздел/ тема дисциплины	Семестр	Аудиторная контактная работа (в акад. часах)			Самостоятельная работа студента	Вид самостоятельной работы	Форма текущего контроля успеваемости и промежуточной аттестации	Код компетенции
		Лек.	лаб. зан.	практ. зан.				
1. Проектирование IoT-систем								
1.1 Принципы построения систем на базе IoT-устройств. Состав IoT систем: сенсоры, актуаторы, гейты	6	3	8		15	Подготовка к практическому занятию. Самостоятельное изучение учебной и научной литературы. Работа с электронными библиотеками. Поиск дополнительной информации по заданной теме	– устный опрос (собеседование); – контрольные работы;	ПК-6.1
1.2 Основные технологии IoT систем. Сбор, передача, хранение и обработка данных. Платформа OPC, протоколы Modbus, облачные платформы, Mesh Network, RTOS, MQTT.		6	12		15	Подготовка к практическому занятию. Самостоятельное изучение учебной и научной литературы. Работа с электронными библиотеками. Поиск дополнительной информации по заданной теме	– устный опрос (собеседование); – контрольные работы;	ПК-6.1
Итого по разделу		9	20		30			
2. Безопасность IoT-систем								

2.1 Архитектура безопасности Интернета вещей. Угрозы и уязвимости информационных систем, содержащих IoT-устройства.	6	4	8		15	Подготовка к практическому занятию. Выполнение индивидуальног о задания Самостоятельное изучение учебной и научной литературы. Работа с электронными библиотеками. Поиск дополнительной информации по заданной теме	– устный опрос (собеседование); – контрольные работы; – индивидуальное задание	ПК-6.1, ПК-6.2, ПК-6.3, ПК-6.4, ПК-7.1, ПК-7.2, ПК-7.3, ПК-7.4
2.2 Моделирование и оценка рисков в Iot-системах, STRIDE.		4	6		11,05	Подготовка к практическому занятию. Выполнение индивидуального задания Самостоятельное изучение учебной и научной литературы. Работа с электронными библиотеками. Поиск дополнительной информации по заданной теме	– устный опрос (собеседование); – контрольные работы; - индивидуальное задание	ПК-6.1, ПК-6.2, ПК-6.3, ПК-6.4, ПК-7.1, ПК-7.2, ПК-7.3, ПК-7.4
Итого по разделу		8	14		26,05			
Итого за семестр		17	34		56,05		зачёт	
Итого по дисциплине		17	34		56,05		зачет	

5 Образовательные технологии

Для реализации предусмотренных видов учебной работы в качестве образовательных технологий в преподавании дисциплины «Безопасность Интернета вещей» используются традиционная и модульно-компетентностная технологии.

Реализация компетентностного подхода предусматривает использование в учебном процессе активных и интерактивных форм проведения занятий в сочетании с внеаудиторной работой с целью формирования и развития профессиональных навыков обучающихся.

При проведении учебных занятий преподаватель обеспечивает развитие у обучающихся навыков командной работы, межличностной коммуникации, принятия решений, лидерских качеств посредством проведения интерактивных лекций, групповых дискуссий, ролевых игр, тренингов, анализа ситуаций , учета особенностей профессиональной деятельности выпускников и потребностей работодателей.

6 Учебно-методическое обеспечение самостоятельной работы обучающихся

Представлено в приложении 1.

7 Оценочные средства для проведения промежуточной аттестации

Представлены в приложении 2.

8 Учебно-методическое и информационное обеспечение дисциплины (модуля)

а) Основная литература:

1.Технологии информационного анализа пользовательского уровня телекоммуникационных систем : Учебное пособие / Котенко Владимир Владимирович ; Южный федеральный университет. - Ростов-на-Дону : Издательство Южного федерального университета (ЮФУ), 2019. - 194 с. - ВО - Специалитет. - URL: https://znanium.com/catalog/document?id=357415 (дата обращения: 27.01.2025)

2. Защита информации : учеб. пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. - 3-е изд. - Москва : РИОР: ИНФРА-М, 2019. - 400 с. - (Высшее образование). - DOI: https://doi.org/10.12737/1759-3. - ISBN 978-5-16-106478-8. - Текст : электронный. - URL: https://znanium.ru/catalog/document?id=443251 (дата обращения: 27.01.2025)

3. Папуловская, Н. В. Основы интернета вещей : Учебно-методическое пособие для студентов инженерно-технических специальностей ИРИТ-РтФ / Н. В. Папуловская ; Министерство науки и высшего образования Российской Федерации, Уральский федеральный университет им. первого Президента России Б.Н. Ельцина. – Екатеринбург : Издательство Уральского университета, 2022. – 104 с. – ISBN 978-5-7996-3537-4. – EDN TQPNUU.

4.Верещагина, Е. А. Проблемы безопасности Интернета вещей / Е. А. Верещагина, И. О. Капецкий, А. С. Ярмонов. – Москва : Общество с ограниченной ответственностью "Издательство "Мир науки", 2021. – 105 с. – ISBN 978-5-6045771-9-6. – EDN DMVFMV.

б) Дополнительная литература:

1. Зараменских, Е. П. Интернет вещей. Исследования и область применения : монография / Е.П. Зараменских, И.Е. Артемьев. — Москва : ИНФРА-М, 2020. - 188 с. — (Научная мысль). — DOI 10.12737/13342. - ISBN 978-5-16-011476-7. - Текст : электронный. - URL: https://znanium.com/catalog/product/1124327 (дата обращения: 27.01.2025)

2. Шелудько, В. М. Язык программирования высокого уровня Python. Функции,

структуры данных, дополнительные модули : учебное пособие / В. М. Шелудько ; Южный федеральный университет. - Ростов-наДону ; Таганрог : Издательство Южного федерального университета, 2017. - 107 с. - ISBN 978-5-9275-2648-2. - Текст : электронный. - URL: https://new.znanium.com/catalog/product/1021664 (дата обращения: 27.01.2025)

3. Коробейников А.Г., Гришенцев А.Ю., Дикий Д.И., Артемьева В.Д., Сидоркина И.Г. Информационная безопасность в системе «Интернет вещей» // Вестник Чувашского университета. – 2018. – № 1. – С. 117–128.

4.Росляков, А. В. Интернет вещей : Учебное пособие / А. В. Росляков, С. В. Ваняшин, А. Ю. Гребешков. – Самара : Поволжский государственный университет телекоммуникаций и информатики, 2015. – 135 с. – EDN ZVDGIL.

в) Методические указания:

1. Методические указания по выполнению лабораторных работ. (Приложение 1.)

2. Методические указания по выполнению внеаудиторных самостоятельных работ. (Приложение 2.)

г) Программное обеспечение и Интернет-ресурсы:

Программное обеспечение

Наименование ПО	№ договора	Срок действия лицензии
7Zip	свободно	бессрочно
Anaconda	свободно	бессрочно
LibreOffice	свободно	бессрочно
Adobe	свободно	бессрочно
Браузер Mozilla	свободно распространя	бессрочно
Браузер	свободно	бессрочно
Calculate Linux	свободно распространя	бессрочно
Arduino	свободно	бессрочно
FAR	свободно	бессрочно
Linux	свободно	бессрочно
NotePad++	свободно	бессрочно

Профессиональные базы данных и информационные справочные системы

Название курса	Ссылка
Информационная система - Нормативные правовые акты, организационно-распоря дительные документы,	https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty-tzi?ysclid=lujknksfy724757053
Информационная система - Банк данных	https://bdu.fstec.ru/?ysclid=lujkqy7cnw630508962

9 Материально-техническое обеспечение дисциплины (модуля)

Материально-техническое обеспечение дисциплины включает:

Материально-техническое обеспечение дисциплины включает:

Лекционные аудитории:
- Мультимедийные средства хранения, передачи и представления информации.

Компьютерные классы:
- Персональные компьютеры с ПО, выходом в Интернет и с доступом в электронную информационно-образовательную среду университета.

Лаборатория защищенных автоматизированных систем:
- Комплект типового учебного оборудования "Сенсор сети zigbee в системе автоматического управления"

Помещения для самостоятельной работы обучающихся:
- Персональные компьютеры с ПО, выходом в Интернет и с доступом в электронную информационно-образовательную среду университета

Приложение 1

Учебно-методическое обеспечение самостоятельной работы обучающихся

Настоящие методические указания предназначены для организации внеаудиторной самостоятельной работы студентов и оказания помощи в самостоятельном изучении теоретического и реализации компетенций обучаемых.

Данные методические указания не являются учебным пособием, поэтому перед началом выполнения самостоятельного задания следует изучить соответствующие разделы лекционных занятий, материалов образовательного портала, разделов основной и дополнительной литературы, представленных в пункте 8. «Учебно-методическое и информационное обеспечение дисциплины (модуля)» данной РПД.

Цели и задачи самостоятельной работы

Цель самостоятельной работы – содействие оптимальному усвоению учебного материала обучающимися, развитие их познавательной активности, готовности и потребности в самообразовании.

Задачи самостоятельной работы:

- повышение исходного уровня владения информационными технологиями;
- углубление и систематизация знаний;
- постановка и решение стандартных задач профессиональной деятельности;
- развитие работы с различной по объему и виду информацией, учебной и научной литературой;
- практическое применение знаний, умений;
- самостоятельно использование стандартных программных средств сбора, обработки, хранения и защиты информации
- развитие навыков организации самостоятельного учебного труда и контроля за его эффективностью.

Виды внеаудиторной самостоятельной работы и формы контроля и время на выполнение каждого вида самостоятельной работы указаны в пункте 4. «Структура и содержание дисциплины» данной РПД.

Порядок выполнения

При выполнении текущей внеаудиторной самостоятельной работы обучающемуся следует придерживаться следующего порядка действий:

1) внимательно изучить соответствующие теоретические разделы дисциплины, пользуясь материалами (лекционными, презентационными, аудио-визуальными):
   а) предоставляемыми преподавателем на лекционных занятиях;

b) предоставляемыми преподавателем в рамках электронных образовательных курсов;
c) содержащимися в учебниках и учебных пособиях ЭБС (электронно-библиотечных систем), электронных каталогов университета и интернет-ресурсов.

2) Подробно разобрать типовые примеры решения задач, рассмотренные в рамках аудиторной контактной работы с преподавателем.
3) Применить полученные теоретические знания и практические навыки к решению индивидуальных заданий, к прохождению компьютерных тестирований.
4) При необходимости, сформировать перечень вопросов, вызвавших затруднения в процессе самостоятельной работы. Обсудить возникшие вопросы со студентами группы, в рамках командно-проектной работы, и с преподавателем, в рамках консультационной помощи, реализованной либо в контактной форме, либо средствами информационно-образовательной среды ВУЗа.

Критерии оценки внеаудиторных самостоятельных работ

Качество выполнения внеаудиторной самостоятельной работы обучающихся оценивается посредством текущего контроля самостоятельной работы обучающихся с использованием балльно-рейтинговой системы.

В качестве форм текущего контроля по дисциплине используются: индивидуальные задания, аудиторные контрольные работы, компьютерное тестирование.

Максимальное количество баллов обучающийся получает, если:

- выполняет индивидуальные задания в соответствии со всеми заявленными требованиями;
- дает правильные формулировки, точные определения, понятия терминов;
- может обосновать рациональность решения текущей задачи.;
- обстоятельно с достаточной полнотой излагает соответствующую теоретический раздел;
- правильно отвечает на дополнительные вопросы преподавателя, имеющие целью выяснить степень понимания им данного материала.

50~85% от максимального количества баллов обучающийся получает, если:

- неполно (не менее 70% от полного), но правильно выполнено задание;
- при изложении были допущены 1-2 несущественные ошибки, которые он исправляет после замечания преподавателя;
- дает правильные формулировки, точные определения, понятия терминов;
- может обосновать свой ответ, привести необходимые примеры;
- правильно отвечает на дополнительные вопросы преподавателя, имеющие целью

выяснить степень понимания им данного материала.

36~50% от максимального количества баллов обучающийся получает, если:

- неполно (не менее 50% от полного), но правильно изложено задание;
- при изложении была допущена 1 существенная ошибка;
- знает и понимает основные положения данной темы, но допускает неточности в формулировке понятий;
- излагает выполнение задания недостаточно логично и последовательно;
- затрудняется при ответах на вопросы преподавателя.

35% и менее от максимального количества баллов обучающийся получает, если:

- неполно (менее 50% от полного) изложено задание;
- при изложении были допущены существенные ошибки. В "0" баллов преподаватель вправе оценить выполненное обучающимся задание, если оно не удовлетворяет требованиям, установленным преподавателем к данному виду работы или не было представлено для проверки.

Сумма полученных баллов по всем видам заданий внеаудиторной самостоятельной работы составляет рейтинговый показатель обучающегося. Рейтинговый показатель обучающегося влияет на выставление итоговой оценки по результатам изучения дисциплины.

Примерные задания и вопросы по темам:

1. Какая технология способна образовывать самоорганизующуюся mesh-сеть по умолчанию, без дополнительных усилий?
2. Концепция построения и развития узкополосных беспроводных сетей связи «Интенета вещей» на территории Российской Федерации
3. Протоколы IPv4 и IPv6
4. Примеры облачных платформ и сервисов для обработки и хранения данных, получаемых от IoT-систем.
5. Протокол MQTT-SN
6. Архитектура IoT-систем
7. Топологии построения сетей ZigBee
8. Датчики технологической информации (температуры, освещенности, присутствия): виды, принцип действия
9. Какие факторы влияют на выбор датчиков при проектировании IoT-систем?
10. Угрозы и уязвимости информационных систем, содержащих IoT-устройства
11. Основные подходы к обеспечению информационной безопасности IoT-систем

Приложение 2

Оценочные средства для проведения промежуточной аттестации

а) Планируемые результаты обучения и оценочные средства для проведения промежуточной аттестации:

Код индикатора	Индикатор достижения компетенции	Оценочные средства
ПК-6 Способен проводить анализ структурных и функциональных схем защищенных автоматизированных информационных систем с целью выявления потенциальных уязвимостей информационной безопасности автоматизированных систем		
ПК-6.1	Проводит анализ структурных и функциональных схем защищенных автоматизированных информационных систем с целью выявления потенциальных уязвимостей информационной безопасности автоматизированных систем	Задание: Разработать систему мониторинга климатических показателей серверного помещения на базе IoT-устройств
ПК-6.2	Выявляет уязвимости информационно-технологических ресурсов автоматизированных систем	1. Уязвимости уровня прикладных программ. 2. Типовые примеры атак на компоненты систем IoT. 3. Канал связи. Проводные и беспроводные сетевые протоколы и их уязвимости.
ПК-6.3	Выявляет основные угрозы безопасности информации в автоматизированных системах	1. Классификация и описание возможных угроз, применительно к области IoT. 2. Риски при использовании устройств IoT. 3. Задание: Построить модель рисков выбранной IoT-системы. Предусмотреть меры по снижению рисков на стадии проектирования системы
ПК-6.4	Составляет протоколы тестирования систем защиты информации автоматизированных систем	Разработать приложения: - приложение имитированного устройства Python - приложение Python для вызова прямых методов на имитированном устройстве. Осуществить управление подключенным к центру Интернета вещей устройством
ПК-7 Способен разрабатывать проектные решения по защите информации в автоматизированных системах		
ПК-7.1	Разрабатывает модели угроз безопасности информации и модели нарушителя в автоматизированных системах	Задание: Разработать модель угроз IoT-системы «Умный дом»
ПК-7.2	Выбирает меры защиты информации, подлежащие	Задание: Составить таблицу рисков на каждом этапе существования данных в

	реализации в системе защиты информации автоматизированной системы	IoT-системе: в процессах, при взаимодействии и хранении. Предложить наилучшие способы их устранения
ПК-7.3	Определяет виды и типы средств защиты информации, обеспечивающих реализацию технических мер защиты информации	1. Применение облачных технологий и сервисно-орентированных архитектур в IoT 2. Обработка данных в IoT 3. Состав IoT-систем 4. Технологии IoT: 2G/3G/4G,5G Спутниковая (VSAT), LPWAN (LORA,LTE-M,NB IOT,NB FI) 5. Услуги инфраструктуры(IaaS), Платформа как услуга(PaaS), услуги программного обеспечения (SaaS). 6. Подключение сенсоров и актуаторов к микроконтроллерам
ПК-7.4	Определяет структуру системы защиты информации автоматизированной системы в соответствии с требованиями нормативных правовых документов в области защиты информации автоматизированных систем	1. Отраслевые сетевые стандарты и модели для IoT под требования безопасности. Задание: Разработать политики безопасности для системы мониторинга климатических показателей на базе IoT-устройств

б) Порядок проведения промежуточной аттестации, показатели и критерии оценивания:

Промежуточная аттестация по дисциплине включает теоретические вопросы, позволяющие оценить уровень усвоения обучающимися знаний, и практические задания, выявляющие степень сформированности умений и владений, проводится в форме экзамена.

Показатели и критерии оценивания экзамена:

– на оценку **«отлично»** (5 баллов) – обучающийся демонстрирует высокий уровень сформированности компетенций, всестороннее, систематическое и глубокое знание учебного материала, свободно выполняет практические задания, свободно оперирует знаниями, умениями, применяет их в ситуациях повышенной сложности.

– на оценку **«хорошо»** (4 балла) – обучающийся демонстрирует средний уровень сформированности компетенций: основные знания, умения освоены, но допускаются незначительные ошибки, неточности, затруднения при аналитических операциях, переносе знаний и умений на новые, нестандартные ситуации.

– на оценку **«удовлетворительно»** (3 балла) – обучающийся демонстрирует пороговый уровень сформированности компетенций: в ходе контрольных мероприятий допускаются ошибки, проявляется отсутствие отдельных знаний, умений, навыков, обучающийся испытывает значительные затруднения при оперировании знаниями и умениями при их переносе на новые ситуации.

– на оценку **«неудовлетворительно»** (2 балла) – обучающийся демонстрирует знания не более 20% теоретического материала, допускает существенные ошибки, не может показать интеллектуальные навыки решения простых задач.

– на оценку **«неудовлетворительно»** (1 балл) – обучающийся не может показать знания на уровне воспроизведения и объяснения информации, не может показать интеллектуальные навыки решения простых задач.