

**ГАОУ ВО «Дагестанский государственный университет на-  
родного хозяйства»**

*Утверждена решением  
Ученого совета ДГУНХ,  
протокол № 11  
от 06 июня 2023 г.*

**Кафедра «Информационные технологии и информационная  
безопасность»**

**РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ  
«БЕЗОПАСНОСТЬ ИНФРАСТРУКТУРЫ ИНТЕРНЕТА-  
ВЕЩЕЙ»**

**Направление подготовки**

**10.04.01 Информационная безопасность,**

**профиль «Управление информационной безопасностью и техно-  
логии защиты информации»**

**Уровень высшего образования - магистратура**

**Форма обучения – очная**

**Махачкала – 2023**

**УДК 681.518(075.8)**

**ББК 32.81.73**

**Составитель** – Гасанова Зарема Ахмедовна, кандидат педагогических наук, заместитель заведующего кафедрой «Информационные технологии и информационная безопасность» ДГУНХ.

**Внутренний рецензент** – Галяев Владимир Сергеевич, кандидат физико-математических наук, доцент, заведующий кафедрой «Информационные технологии и информационная безопасность» ДГУНХ.

**Внешний рецензент** – Абдурагимов Гусейн Эльдарханович, кандидат физико-математических наук, доцент кафедры прикладной математики Дагестанского государственного университета.

**Представитель работодателя** - Зайналов Джабраил Тажутдинович, директор регионального экспертно-аттестационного центра «Экспертиза», эксперт-представитель работодателя.

*Рабочая программа дисциплины «Безопасность инфраструктуры Интернета-вещей» разработана в соответствии с требованиями федерального государственного образовательного стандарта высшего образования по направлению подготовки 10.04.01 Информационная безопасность, утвержденного приказом Министерства образования и науки Российской Федерации от 26 ноября 2020 г., № 1455, в соответствии с приказом Министерства науки и высшего образования от 6.04.2021 г., № 245 «Об утверждении Порядка организации и осуществления образовательной деятельности по образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры»*

Рабочая программа по дисциплине «Безопасность инфраструктуры Интернета-вещей» размещена на официальном сайте [www.dgunh.ru](http://www.dgunh.ru)

Гасанова З.А. Рабочая программа по дисциплине «Безопасность инфраструктуры Интернета-вещей» для направления подготовки 10.04.01 Информационная безопасность, профиль «Управление информационной безопасностью и технологии защиты информации». – Махачкала: ДГУНХ, 2023 г., 13 с.

Рекомендована к утверждению Учебно-методическим советом ДГУНХ 05 июня 2023 г.

Рекомендована к утверждению руководителем основной профессиональной образовательной программы высшего образования – программы бакалавриата по направлению подготовки 10.03.01 Информационная безопасность, профиль «Безопасность автоматизированных систем», к.пед.н., Гасановой З.А.

Одобрена на заседании кафедры «Информационные технологии и информационная безопасность» 31 мая 2023 г., протокол № 10.

## Содержание

Раздел 1. Перечень планируемых результатов обучения по дисциплине...	4
Раздел 2. Место дисциплины в структуре образовательной программы...	6
Раздел 3. Объем дисциплины в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий), на самостоятельную работу обучающихся и форму(ы) промежуточной аттестации.....	6
Раздел 4. Содержание дисциплины, структурированное по темам с указанием отведенного на них количества академических часов и видов учебных занятий.....	7
Раздел 5. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины.....	9
Раздел 6. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины.....	10
Раздел 7. Перечень лицензионного программного обеспечения, информационных справочных систем и профессиональных баз данных.....	11
Раздел 8. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине.....	11
Раздел 9. Образовательные технологии.....	12
Лист актуализации рабочей программы дисциплины.....	13

## Раздел 1. Перечень планируемых результатов обучения по дисциплине

Цель дисциплины – сформировать компетенции обучающегося в области использования особенностей информационных технологий, применяемых в автоматизированных системах, при организации защиты обрабатываемой в них информации.

Задачами преподавания дисциплины являются:

- изучение понятийного аппарата дисциплины, основных теоретических положений и методов;
- формирование умений и привитие навыков применения теоретических знаний для решения практических и прикладных задач.

### 1.1. Компетенции выпускников, формируемые в результате освоения дисциплины «Безопасность инфраструктуры Интернета-вещей» как часть планируемых результатов освоения образовательной программы

код компетенции	формулировка компетенции
ПК-1.	Способен осуществлять подбор средств и технологий защиты информации и применять их в профессиональной деятельности

### 1.2. Планируемые результаты обучения по дисциплине

<i>Код и наименование компетенции</i>	<i>Код и наименование индикатора достижения компетенции</i>	<i>Планируемые результаты обучения по дисциплине</i>
ПК-1. Способен осуществлять подбор средств и технологий защиты информации и применять их в профессиональной деятельности	ПК-1.2. Обеспечивает безопасность применяемых информационных технологий	<b><u>Знать:</u></b> <ul style="list-style-type: none"><li>- способы формирования требований к кибербезопасности (информационной безопасности) систем «Интернета вещей»;</li><li>- основные направления деятельности по обеспечению безопасности Интернета вещей, объектов критической информационной инфраструктуры;</li><li>- требования нормативно-правовых актов и стандартов по разработке моделей угроз информационной безопасности</li></ul> <b><u>Уметь:</u></b> <ul style="list-style-type: none"><li>- использовать средства и технологии защиты от основных угроз, уязвимо-</li></ul>

		<p>стей, рисков в области безопасности Интернета вещей, в составе объектов критической информационной инфраструктуры;</p> <ul style="list-style-type: none"> <li>- использовать технологии предотвращения угроз сетевой безопасности, а также механизмы противодействия сетевым атакам;</li> <li>- проектировать систему безопасности объектов критической информационной инфраструктуры</li> </ul> <p><b><u>Владеть:</u></b></p> <ul style="list-style-type: none"> <li>- навыками работы по разработке планов и проведению мероприятий по организации защиты информации (обеспечению кибербезопасности) систем «Интернета вещей», объектов КИИ в организации;</li> <li>- навыками работы по построению и проверки моделей анализа и синтеза инфокоммуникационных систем, сетей и устройств</li> </ul>
--	--	---

### 1.3. Перечень компетенций с указанием этапов их формирования в процессе освоения дисциплины

Код компетенции	Этапы формирования компетенций			
	Тема 1. Введение в проблему информационной безопасности Интернета вещей, области применения, специфика требований.	Тема 2. Жизненный цикл проекта Интернета вещей	Тема 3. Классификация систем Интернета вещей. Нормативно-правовое регулирование. Требования к обеспечению информационной безопасности.	Тема 4. Обзор существующих методов защиты систем промышленных предприятия, требования и особенности интеграции элементов и систем защиты информации.
ПК-1	+	+	+	+

Код компетенции	Этапы формирования компетенций		
	Тема 5 Управление рисками в системах интернета вещей. Классификация рисков, построение модели угроз. Критерии достаточности в управлении рисками Управление рисками как услуга: критерии качества	Тема 6. Понятие модели нарушителя, отраслевые модели нарушителя Влияние модели нарушителя на процесс разработки прикладного программного обеспечения	Тема 7. Методы снижения полной стоимости системы защиты информации.
ПК-1	+	+	+

## **Раздел 2. Место дисциплины в структуре образовательной программы**

Дисциплина Б1.В.ДВ.03.01 «Безопасность инфраструктуры Интернета вещей» относится к дисциплинам по выбору Блока 1 «Дисциплины» учебного плана направления подготовки «Информационная безопасность», профиля «Управление информационной безопасностью и технологии защиты информации».

Для изучения данной дисциплины необходимы знания, умения и навыки по дисциплинам: «Технологии обеспечения информационной безопасности», «Защищенные информационные системы», «Экономика защиты информации», «Управление информационной безопасностью».

Освоение данной дисциплины необходимо обучающемуся для успешного прохождения практик и выполнения выпускной квалификационной работы.

## **Раздел 3. Объем дисциплины в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий), на самостоятельную работу обучающихся, на самостоятельную работу обучающихся и форму промежуточной аттестации**

Объем дисциплины в зачетных единицах составляет 5 зачетных единиц.

Очная форма обучения

Количество академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий), составляет 72 часа, в том числе:

на занятия лекционного типа – 36 ч.

на занятия семинарского типа – 36 ч.

Количество академических часов, выделенных на самостоятельную работу обучающихся – 72 ч.

Форма промежуточной аттестации: экзамен, 36 ч.

**Раздел 4. Содержание дисциплины, структурированное по темам с указанием отведенного на них количества академических часов и видов учебных занятий.**

**Очная форма обучения**

№ п/п	Тема дисциплины	Всего академических часов	В т.ч. занятия лекционного типа	В т.ч. занятия семинарского типа:					Самостоятельная работа	Форма текущего контроля успеваемости. Форма промежуточной аттестации
				семинары	Практические занятия	Лабораторные занятия (лабораторные работы, лабораторный практикум)	Коллоквиумы	Иные аналогичные занятия		
1.	Тема 1. Введение в проблему информационной безопасности Интернета вещей, области применения, специфика требований.	18	4	-	2	2	-	-	10	<ul style="list-style-type: none"> <li>- Устный опрос</li> <li>- Подготовка реферата;</li> <li>- Подготовка презентации;</li> <li>- Тестирование;</li> <li>- Практическая работа;</li> <li>- Лабораторная работа.</li> </ul>
2.	Тема 2. Жизненный цикл проекта Интернета вещей	18	4	-	2	2	-	-	10	<ul style="list-style-type: none"> <li>- Устный опрос</li> <li>- Подготовка реферата;</li> <li>- Подготовка презентации;</li> <li>- Тестирование;</li> <li>- Практическая работа;</li> <li>- Лабораторная работа.</li> </ul>
3.	Тема 3. Классификация систем Интернета вещей. Нормативно-правовое регулирование. Требования к обеспечению информационной безопасности.	20	6	-	2	2	-	-	10	<ul style="list-style-type: none"> <li>- Устный опрос</li> <li>- Подготовка реферата;</li> <li>- Подготовка презентации;</li> <li>- Тестирование;</li> <li>- Практическая работа;</li> <li>- Лабораторная работа.</li> </ul>
4.	Тема 4. Обзор существующих методов защиты систем промышленных предприятия, требования и особенности интеграции элементов и систем защиты информации.	18	4	-	2	2	-	-	10	<ul style="list-style-type: none"> <li>- Устный опрос</li> <li>- Подготовка реферата;</li> <li>- Подготовка презентации;</li> <li>- Тестирование;</li> <li>- Практическая работа;</li> <li>- Лабораторная работа.</li> </ul>

5.	Тема 5 Управление рисками в системах интернета вещей. Классификация рисков, построение модели угроз. Критерии достаточности в управлении рисками Управление рисками как услуга: критерии качества	20	6	-	2	2	-	-	10	<ul style="list-style-type: none"> <li>- Устный опрос</li> <li>- Подготовка реферата;</li> <li>- Подготовка презентации;</li> <li>- Тестирование;</li> <li>- Практическая работа;</li> <li>- Лабораторная работа.</li> </ul>
6.	Тема 6. Понятие модели нарушителя, отраслевые модели нарушителя Влияние модели нарушителя на процесс разработки прикладного программного обеспечения	24	6	-	4	4	-	-	10	<ul style="list-style-type: none"> <li>- Устный опрос</li> <li>- Подготовка реферата;</li> <li>- Подготовка презентации;</li> <li>- Тестирование;</li> <li>- Практическая работа;</li> <li>- Лабораторная работа.</li> </ul>
7.	Тема 7. Методы снижения полной стоимости системы защиты информации.	26	6	-	4	4	-	-	12	<ul style="list-style-type: none"> <li>- Устный опрос</li> <li>- Подготовка реферата;</li> <li>- Подготовка презентации;</li> <li>- Тестирование;</li> <li>- Практическая работа;</li> <li>- Лабораторная работа.</li> </ul>
<b>ИТОГО</b>		<b>0</b>	<b>0</b>	<b>-</b>	<b>0</b>	<b>18</b>	<b>-</b>	<b>-</b>	<b>0</b>	
<b>Экзамен (групповая консультация в течение семестра, групповая консультация перед промежуточной аттестацией, экзамен)</b>		<b>36</b>								Контроль
<b>ИТОГО</b>		<b>180</b>								

**Раздел 5. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины**

№ п/п	Автор	Название основной и дополнительной учебной литературы, необходимой для освоения дисциплины	Выходные данные	Количество экземпляров в библиотеке ДГУНХ/ адрес доступа
<b>I. Основная учебная литература</b>				
1.	Вагин Д. В.	Современные технологии разработки веб-приложений	Учебное пособие : [16+] / Д. В. Вагин, Р. В. Петров ; Новосибирский государственный технический университет. – Новосибирск : Новосибирский государственный технический университет, 2019. – 52 с.	<a href="https://biblioclub.ru/index.php?page=book&amp;id=573960">https://biblioclub.ru/index.php?page=book&amp;id=573960</a>
2.	Сычев А. В.	Перспективные технологии и языки веб-разработки	А. В. Сычев. – 2-е изд., испр. – Москва : Национальный Открытый Университет «ИНТУ-ИТ», 2016. – 494 с.	<a href="https://biblioclub.ru/index.php?page=book&amp;id=429078">https://biblioclub.ru/index.php?page=book&amp;id=429078</a>
<b>II. Дополнительная литература</b>				
<b>A) Дополнительная учебная литература</b>				
1.	Богданов М. Р.	Перспективные языки веб-разработки	/ М. Р. Богданов. – 2-е изд., испр. – Москва : Национальный Открытый Университет «ИНТУ-ИТ», 2016. – 265 с.	<a href="https://biblioclub.ru/index.php?page=book&amp;id=428953">https://biblioclub.ru/index.php?page=book&amp;id=428953</a>
2.	Маркин А. В.	Основы web-программирования на PHP :	Учебное пособие / А. В. Маркин, С. С. Шкарин. – Москва : Диалог-МИФИ, 2012. – 252 с.	<a href="https://biblioclub.ru/index.php?page=book&amp;id=229742">https://biblioclub.ru/index.php?page=book&amp;id=229742</a>

<b>Б) Официальные издания: сборники законодательных актов, нормативно-правовых документов и кодексов РФ</b>	
1.	Федеральный закон от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации" (с изменениями и дополнениями).
2.	ГОСТ Р 50922-2006. Защита информации. Основные термины и определения. 2008 г. <a href="http://www.standartgost.ru">www.standartgost.ru</a>
3.	ГОСТ Р ИСО/МЭК 17799-2005. Информационная технология. Практические правила управления информационной безопасностью. <a href="http://www.standartgost.ru">www.standartgost.ru</a>
4.	ГОСТ Р ИСО/МЭК 15026-2002. Информационная технология. Уровни целостности систем и программных средств. 2002 г. <a href="http://www.standartgost.ru">www.standartgost.ru</a>
<b>В) Периодические издания</b>	
1.	Журнал для пользователей персональных компьютеров «Мир ПК»
2.	Научный журнал «Информатика и ее применение»
3.	Информатика и безопасность
4.	Журнал о компьютерах и цифровой технике «Computer Bild»
5.	Рецензируемый научный журнал «Информатика и система управления»
6.	Рецензируемый научный журнал «Проблемы информационной безопасности»
<b>Г) Справочно-библиографическая литература</b>	
1.	1. Краткий энциклопедический словарь по информационной безопасности : словарь / сост. В.Г. Дождиков, М.И. Салтан. – Москва : Энергия, 2010. – 240 с. <a href="http://biblioclub.ru/index.php?page=book&amp;id=58393">http://biblioclub.ru/index.php?page=book&amp;id=58393</a>

## **Раздел 6. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины**

Каждый обучающийся в течение всего периода обучения обеспечен индивидуальным неограниченным доступом к одной или нескольким электронно-библиотечным системам и к электронной информационно-образовательной среде университета (<http://e-dgunh.ru>). Электронно-библиотечная система и электронная информационно-образовательная среда обеспечивает возможность доступа, обучающегося из любой точки, в которой имеется доступ к информационно-телекоммуникационной сети "Интернет", как на территории университета, так и вне ее.

Для самостоятельного изучения материала и ознакомления с регламентирующими документами и текущей практикой в области защиты информации, рекомендуется использовать следующие Интернет-ресурсы:

1. <http://www.fsb.ru/> – официальный сайт ФСБ
2. <http://fstec.ru/> – официальный сайт ФСТЭК
3. <http://www.consultant.ru/> – онлайн-версия информационно-правовой системы "КонсультантПлюс"

4. <http://Standartgost.ru> - Открытая база ГОСТов

## **Раздел 7. Перечень лицензионного программного обеспечения, информационных справочных систем и профессиональных баз данных**

### **7.1. Лицензионное и свободно распространяемое программное обеспечение, в том числе отечественного производства**

- Windows 10
- Microsoft Office Professional
- Adobe Acrobat Reader DC
- VLC Media player
- 7-zip

### **7.2. Перечень информационных справочных систем и профессиональных баз данных:**

- информационно справочная система «КонсультантПлюс».

### **7.3. Перечень профессиональных баз данных:**

- Государственный реестр сертифицированных средств защиты информации N РОСС RU.0001.01БИ00 (<http://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty-po-sertifikatsii/153-sistema-sertifikatsii/591-gosudarstvennyj-reestr-sszi>).
- <http://Standartgost.ru> - Открытая база ГОСТов.

## **Раздел 8. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине**

Для преподавания дисциплины «Безопасность инфраструктуры Интернета-вещей» используются следующие специальные помещения и учебные аудитории:

**Учебная аудитория для проведения учебных занятий № 4.10 (Россия, Республика Дагестан, 367008, г. Махачкала, ул. Джамалутдина Атаева, дом 5, учебный корпус № 2 литер «В»)**

### ***Перечень основного оборудования:***

Комплект специализированной мебели.

Доска меловая.

Набор демонстрационного оборудования: проектор, персональный компьютер с доступом к сети Интернет и корпоративной сети университета, ЭБС «Университетская библиотека ONLINE» ([www.biblioclub.ru](http://www.biblioclub.ru)), ЭБС «ЭБС Юрайт» ([www.urait.ru](http://www.urait.ru)), интерактивная доска, акустическая система.

### ***Перечень учебно-наглядных пособий:***

Комплект наглядных материалов (баннеры, плакаты);

Комплект электронных иллюстративных материалов (презентации, видеоролики).

**Лаборатория сетей и систем передачи информации, учебная аудитория для проведения учебных занятий № 4.8(Россия, Республика Дагестан, 367008, г. Махачкала, ул. Джамалутдина Атаева, дом 5, учебный корпус № 2 литер «В»)**

### ***Перечень основного оборудования:***

Комплект специализированной мебели.

Доска меловая.

Набор демонстрационного оборудования: проектор, акустическая система.

Персональные компьютеры – 20 ед.

***Перечень учебно-наглядных пособий:***

Комплект наглядных материалов (баннеры, плакаты);

Комплект электронных иллюстративных материалов (презентации, видеоролики).

**Помещение для самостоятельной работы № 4.5 (Россия, Республика Дагестан, 367008, г. Махачкала, ул. Джамалутдина Атаева, дом 5, учебный корпус № 2 литер «В»)**

***Перечень основного оборудования:***

Персональные компьютеры с доступом к сети «Интернет» и в электронную информационно-образовательную среду – 19 ед.

**Помещение для самостоятельной работы № 1-1 (Россия, Республика Дагестан, 367008, г. Махачкала, ул. Джамалутдина Атаева, дом 5, учебный корпус № 1)**

***Перечень основного оборудования:***

Персональные компьютеры с доступом к сети «Интернет» и в электронную информационно-образовательную среду – 60 ед.

## **Раздел 9. Образовательные технологии**

Образовательные технологии, используемые при проведении учебных занятий по дисциплине «Безопасность инфраструктуры Интернета-вещей», обеспечивают развитие у обучающихся необходимых знаний и навыков.

На занятиях лекционного типа применяются такие методы обучения как управляемая дискуссия, проблемная лекции, техники сторителлинга.

На практических занятиях, целью которых является приобретение учащимися определенных практических умений, научить их аналитически мыслить, уметь принимать верные решения в различных ситуациях эффективными будут такие методы как решение задач, выполнение лабораторных работ.

**Лист актуализации рабочей программы дисциплины**  
**«Безопасность инфраструктуры Интернета-вещей»**

Рабочая программа пересмотрена,  
обсуждена и одобрена на заседании кафедры

Протокол от «\_\_\_\_\_» \_\_\_\_\_ 20\_\_ г. № \_\_\_\_\_

Зав. кафедрой \_\_\_\_\_

Рабочая программа пересмотрена,  
обсуждена и одобрена на заседании кафедры

Протокол от «\_\_\_\_\_» \_\_\_\_\_ 20\_\_ г. № \_\_\_\_\_

Зав. кафедрой \_\_\_\_\_

Рабочая программа пересмотрена,  
обсуждена и одобрена на заседании кафедры

Протокол от «\_\_\_\_\_» \_\_\_\_\_ 20\_\_ г. № \_\_\_\_\_

Зав. кафедрой \_\_\_\_\_

Рабочая программа пересмотрена,  
обсуждена и одобрена на заседании кафедры

Протокол от «\_\_\_\_\_» \_\_\_\_\_ 20\_\_ г. № \_\_\_\_\_

Зав. кафедрой \_\_\_\_\_