
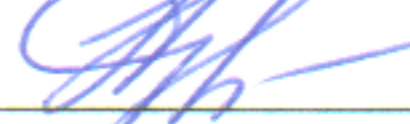


Министерство науки и высшего образования Российской Федерации  
ФГБОУ ВО «Дагестанский государственный технический университет»

РЕКОМЕНДОВАНО  
К УТВЕРЖДЕНИЮ  
Декан, председатель совета  
факультета КТВТиЭ

  
Ш. А. Юсуфов  
« 17 » 10 20 18 г.

УТВЕРЖДАЮ  
Проректор по учебной работе,  
председатель методического  
совета ДГТУ

  
Н. С. Суракатов  
« 22 » 10 20 18 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЬ)

Дисциплина Б1.В.ОД.5 Технология построения защищенных АС

Направление 10.03.01 – Информационная безопасность

Профиль Безопасность автоматизированных систем

Факультет Компьютерных технологий, вычислительной техники и энергетики  
наименование факультета, где ведется дисциплина

Кафедра Информационная безопасность  
наименование кафедры, за которой закреплена дисциплина

Квалификация выпускника бакалавр

Форма обучения очная; курс 4; семестр 7;

Всего трудоемкость в зачетных единицах (часах) 53ЕТ (180 ч)

Лекции 34 (час): экзамен 7 семестр (1зет=36ч)

практические (семинарские) занятия - (час): зачет - (семестр)

лабораторные занятия 34 (час): самостоятельная работа 76 (час):

курсовой проект (работа, РГР) - (семестр).


Зав. кафедрой ИБ   
подпись Г.И. Качаева

Начальник УО   
подпись Э.В. Магомаева



Программа составлена в соответствии с требованиями ФГОС ВО с учетом рекомендаций ООП ВО по направлению 10.03.01 – «Информационная безопасность», профиль «Безопасность автоматизированных систем».


Программа одобрена на заседании выпускающей кафедры ИБ от 15.10.2018г., протокол № 2

Зав. выпускающей кафедрой по данному направлению  Г.И.Качаева

**ОДОБРЕНО**

Методической комиссией по  
укрупненным группам  
специальностей и направлению  
подготовки  
10.00.00- «Информационная  
безопасность»

**Председатель МК**

  
Мелехин В.Б.  
подпись ИОФ

«15» 10 2018г.

**АВТОР ПРОГРАММЫ**

Качаева Г.И., к.э.н., ст. преп. каф. ИБ  
И.О.Ф. уч. степень, ученое звание, подпись



## 1. Цели и задачи дисциплины

### 1.1 Цели дисциплины

Целью дисциплины «Технология построения защищенных автоматизированных систем» является формирование у студентов знаний основ технологии построения, проектирования и создания защищенных автоматизированных систем, а также навыков и умения в применении знаний для конкретных условий. Кроме того, целью дисциплины является развитие в процессе обучения системного мышления, необходимого для решения задач защиты информации с учетом требований системного подхода.

### 1.2 Задачи дисциплины

Задачи изучения дисциплины:

- концепции обеспечения информационной безопасности автоматизированных систем;
- технологии функционирования защищенной автоматизированной системы;
- методологии оценки защищенности автоматизированных систем;
- принципов построения защищенных информационных систем;

## 2. Место дисциплины в структуре ООП бакалавриата

Дисциплина «Технология построения защищенных АС» относится к вариативной части ФГОС ВО.

Предшествующими дисциплинами, формирующими начальные знания, являются следующие дисциплины: языки программирования.

Последующими дисциплинами являются: Защита программ и данных

## 3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующей компетенции:

способностью понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации (ОПК-4);

способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты (ОПК-7).

В результате изучения дисциплины студент должен

**Знать:** средства и методы предотвращения и обнаружения вторжений; технические каналы утечки информации; возможности технических средств перехвата информации; способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации; организацию защиты информации от утечки по техническим каналам на объектах информатизации;

**Уметь:** пользоваться нормативными документами по противодействию технической разведке; оценивать качество готового программного обеспечения;

**Владеть:** методами и средствами технической защиты информации; методами расчета и инструментального контроля показателей технической защиты информации.

#### 4. Структура и содержание дисциплины «Технология построения защищенных АС»

Общая трудоемкость дисциплины составляет 5 зачетных единиц – 180 часа, в том числе: лекционных -34 часов, лабораторных - 34 часов, СРС – 76 часов, форма отчетности экзамен в 7 семестре.

##### 4.1.Содержание дисциплины

№ п/п	Раздел дисциплины Тема лекции и вопросы	Семестр Неделя/семестра	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)				Формы текущего* контроля успеваемости (по срокам текущих аттестаций в семестре)
			ЛК	ПЗ	ЛР	СР	
1.	<b>Лекция №1</b> <b>Тема: «Системный подход к построению защищенных автоматизированных систем».</b> Понятие сложной системы. Управление и информация, самоорганизация. Основные принципы системного подхода при создании сложных систем; Понятие качества и эффективности.	1.2	4		4	8	Вх. Контр.
2.	<b>Лекция №2</b> <b>Тема: «Оценка эффективности сложных систем»</b> Методические вопросы оценки эффективности сложных систем. Функциональная и обеспечивающая часть сложной системы. Технология функционирования сложной системы	3.4	4		4	8	
3.	<b>Лекция № 3</b> <b>Тема: «Проектирование автоматизированных систем»</b> Цели и задачи проектирования. Структуризация предметной области. Классификация объектов проектирования. Жизненный цикл автоматизированной системы. Этапы <sup>5</sup> проектирования системы. Организация работ, функции заказчиков и разработчиков.	5.6	4		4	8	АКР №1
4.	<b>Лекция №4</b> <b>Тема: «Проектирование и построение системы защиты автоматизированных систем»</b> Практические методы реализации моделей безопасности. Ядра безопасности. Мониторинг взаимодействий в системе. Архитектура защищенных систем. Принципы построения защищенных информационных систем. Технологический цикл реализации защищенной системы обработки и хранения информации. Реализация систем контроля доступа; способы представления информации о правах доступа.	7.8	4		4	8	
5.	<b>Лекция № 5</b> <b>Тема: «Методология оценки защищенности изделий и продуктов информационных технологий»</b> Критерии оценки безопасности информационных	9.10	4		4	8	АКР №2

	технологий. Контекст безопасности. Профиль защиты и задание по безопасности. Функциональные требования безопасности.						
6.	<b>Лекция № 6</b> <b>Тема: «Использование защищенных компьютерных систем»</b> Защищенные компьютерные системы. Их виды и особенности. Примеры защищенных систем. Их использование и применение на практике.	11.12	4		4	10	
7.	<b>Лекции № 7</b> <b>Тема: «Критерии качества»</b> Определение критериев качества для конкретных изделий и продуктов информационных технологий (ИТ). Сравнение изделий и продуктов ИТ по критериям качества.	13.14	4		4	10	
8.	<b>Лекция №8</b> <b>Тема: «Структура формирования проекта»</b> Создание проекта изделия ИТ: документооборот в локальной сети предприятия. Создание проекта изделия ИТ: документооборот в глобальной сети предприятия.	15.16	4		4	8	АКР №3
9.	<b>Лекция №9</b> <b>Тема: «Защита документооборота»</b> Подготовка профиля защиты и задание по безопасности изделия ИТ: защищенный документооборот в локальной сети предприятия. Подготовка профиля защиты и задание по безопасности изделия ИТ: защищенный документооборот в глобальной сети предприятия.	17	2		2	8	
<b>Итого по дисциплине</b>			<b>34</b>		<b>34</b>	<b>76</b>	<b>Экзамен (1зет=36ч)</b>

## 4.2. Содержание лабораторных занятий

№ п/п	№ лекции израбоче й програм мы	Наименование лабораторного (практического, семинарского) занятия	Рекомендуема я литература и методические разработки (№ источника из списка литературы)	Кол-во часов
1	Лк №1	«Системный подход к построению защищенных автоматизированных систем»	№№ 1-10	4
2	Лк №2	«Оценка эффективности сложных систем»	№№ 1-10	4
3	Лк №3	«Проектирование автоматизированных систем»	№№ 1-10	4
4	Лк № 4	«Проектирование и построение системы защиты автоматизированных систем»	№№ 1-10	4
5	Лк № 5	«Методология оценки защищенности изделий и продуктов информационных технологий»	№№ 1-10	4
6	Лк №6	«Использование защищенных компьютерных систем»	№№ 1-10	4
7	Лк № 7	«Критерии качества»	№№ 1-10	4
8	Лк №8	«Структура формирования проекта»	№№ 1-10	4
9	Лк №8	«Защита документооборота»	№№ 1-10	2
<b>Итого по дисциплине</b>				<b>34</b>

## 4.3. Тематика для самостоятельной работы студента

### 4.4.

№ п/п	Тематика по содержанию дисциплины, выделенная для самостоятельного изучения	Кол-во часов из содержания дисциплины	Рекоменду емая литература и источники информаци и	Форма контрол я СРС
1.	«Системный подход к построению защищенных автоматизированных систем»	8	№№ 1-10	Опрос, реферат, статья
2.	«Оценка эффективности сложных систем»	8	№№ 1-10	Опрос, реферат, статья
3.	«Проектирование автоматизированных систем»	8	№№ 1-10	Опрос, реферат, статья
4.	«Проектирование и построение системы защиты автоматизированных систем»	8	№№ 1-10	Опрос, реферат, статья
5.	«Методология оценки защищенности изделий и продуктов информационных технологий»	8	№№ 1-10	Опрос, реферат, статья

	технологий»			
6.	«Использование защищенных компьютерных систем»	10	№№ 1-10	Опрос, реферат, статья
7.	«Критерии качества»	10	№№ 1-10	Опрос, реферат, статья
8.	«Структура формирования проекта»	8	№№ 1-10	Опрос, реферат, статья
9.	«Защита документооборота»	8	№№ 1-10	Опрос, реферат, статья
<b>Итого</b>		<b>76</b>		

## **5. Образовательные технологии**

В соответствии с требованиями ФГОС ВО по направлению подготовки реализация компетентностного подхода должна предусматривать широкое использование в учебном процессе активных и интерактивных форм проведения занятий в сочетании с внеаудиторной работой с целью формирования и развития профессиональных навыков обучающихся.

Удельный вес занятий, проводимых в интерактивных формах, определяется главной целью программы, особенностью контингента обучающихся и содержанием дисциплины, и в целом в учебном процессе они составляют не менее 20% аудиторных занятий.

При проведении занятий по учебной дисциплине рекомендуется следовать и традиционным технологиям, в частности, в каждом разделе курса выделять наиболее важные моменты, акцентировать на них внимание обучаемых.

При чтении лекций по всем разделам программы иллюстрировать теоретический материал большим количеством примеров, что позволит сделать изложение наглядным и продемонстрировать обучаемым приемы программирования.

При изучении всех разделов программы добиться точного знания обучаемыми основных исходных понятий.

## **6. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины и учебно-методическое обеспечение самостоятельной работы студентов**

### **Вопросы входного контроля для проверки знаний студентов**

1. Что такое программное обеспечение?
2. Жизненный цикл программного обеспечения.
3. Модели разработки программного обеспечения
4. Объектно-ориентированный подход.
5. Модель «водопада» разработки программного обеспечения.
6. Определение, краткая характеристика. Агрегацией и композиция классов.
7. Понятия и соотношение. Интерфейсы. Проектирование классов. Структура класса.
8. Диаграммы состояний объекта. Способы проектирование методов класса. Парадигмы программирования: визуальная, функциональная, процедурная, объектно-ориентированная и т.д.

9. Объектно-ориентированная парадигма: понятия объекта, класса объектов; основные понятия объектно-ориентированного программирования (инкапсуляция, наследование и полиморфизм); классы и объекты; интерфейсы и реализация.

### **Контрольные вопросы для проверки текущих знаний студентов**

#### **Аттестационная контрольная работа №1**

1. Понятие сложной системы.
2. Управление и информация, самоорганизация.
3. Основные принципы системного подхода при создании сложных систем;
4. Понятие качества и эффективности.
5. Методические вопросы оценки эффективности сложных систем.
6. Функциональная и обеспечивающая часть сложной системы.
7. Технология функционирования сложной системы
8. Цели и задачи проектирования.
9. Структуризация предметной области.
10. Классификация объектов проектирования.
11. Жизненный цикл автоматизированной системы.

#### **Аттестационная контрольная работа №2**

1. Практические методы реализации моделей безопасности.
2. Ядра безопасности.
3. Мониторинг взаимодействий в системе.
4. Архитектура защищенных систем.
5. Принципы построения защищенных информационных систем.
6. Технологический цикл реализации защищенной системы обработки и хранения информации.
7. Реализация систем контроля доступа; способы представления информации о правах доступа.
8. Критерии оценки безопасности информационных технологий.
9. Контекст безопасности.
10. Профиль защиты и задание по безопасности. Функциональные требования безопасности.

#### **Аттестационная контрольная работа №3**

1. Защищенные компьютерные системы.
2. Их виды и особенности.
3. Примеры защищенных систем. Их использование и применение на практике.
4. Определение критериев качества для конкретных изделий и продуктов информационных технологий (ИТ).
5. Сравнение изделий и продуктов ИТ по критериям качества.
6. Создание проекта изделия ИТ: документооборот в локальной сети предприятия.
7. Создание проекта изделия ИТ: документооборот в глобальной сети предприятия.

#### **Перечень вопросов на экзамен**

1. Понятие сложной системы.
2. Управление и информация, самоорганизация.
3. Основные принципы системного подхода при создании сложных систем;
4. Понятие качества и эффективности.
5. Методические вопросы оценки эффективности сложных систем.



6. Функциональная и обеспечивающая часть сложной системы.
7. Технология функционирования сложной системы
8. Цели и задачи проектирования.
9. Структуризация предметной области.
10. Классификация объектов проектирования.
11. Жизненный цикл автоматизированной системы.
12. Практические методы реализации моделей безопасности.
13. Ядра безопасности.
14. Мониторинг взаимодействий в системе.
15. Архитектура защищенных систем.
16. Принципы построения защищенных информационных систем.
17. Технологический цикл реализации защищенной системы обработки и хранения информации.
18. Реализация систем контроля доступа; способы представления информации о правах доступа.
19. Критерии оценки безопасности информационных технологий.
20. Контекст безопасности.
21. Профиль защиты и задание по безопасности. Функциональные требования безопасности.
22. Защищенные компьютерные системы.
23. Их виды и особенности.
24. Примеры защищенных систем. Их использование и применение на практике.
25. Определение критериев качества для конкретных изделий и продуктов информационных технологий (ИТ).
26. Сравнение изделий и продуктов ИТ по критериям качества.
27. Создание проекта изделия ИТ: документооборот в локальной сети предприятия.
28. Создание проекта изделия ИТ: документооборот в глобальной сети предприятия.

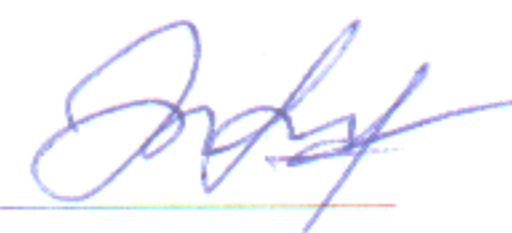
### **Вопросы проверки остаточных знаний**

1. Структуры данных
2. Динамические структуры данных
3. Деревья
4. Алгоритмы
5. Алгоритмы на графах
6. Алгоритмы сортировки
7. Алгоритмы поиска
8. Технологии проектирования и программирования
9. Объектно-ориентированный подход к разработке ПО
10. Технология создания программного кода»
11. Технологии коллективной разработки программного обеспечения
12. Технологические средства разработки программного обеспечения
13. Методы отладки и тестирования программ
14. Документирование и оценка качества программных продуктов

7. Учебно-методическое и информационное обеспечение дисциплины (модуля)  
«Технология построения защищенных АС»

7.1. Рекомендуемая литература и источники информации

Зав. библиотекой \_\_\_\_\_



№	Виды занятий (лк, пр, лб, ср)	Комплект необходимой учебной лит-ры по дисциплинам (наименование учебника, пособия)	Авторы	Издат-во и год издания	Кол-во пособий, учебников и прочей литературы	
					в библ	на каф
<b>О С Н О В Н А Я</b>						
1.	Лк, лб, ср	Разработка системы технической защиты информации	Аверченков В.И.	ФЛИНТА, 2011. - 187 с	<a href="http://znanium.com/bookread.php?book=453880">http://znanium.com/bookread.php?book=453880</a>	
2.	Лк, пр, ср	Информационная безопасность и защита информации	Шаньгин, В. Ф.	Электрон. текстовые дан. – Москва : ДМК Пресс, 2014. – 702 с	<a href="http://www.iprbbookshop.ru/29257">http://www.iprbbookshop.ru/29257</a>	
3.	Лк, пр, ср	Универсальное кодирование. Теория и алгоритмы	Штарьков, Ю. М.	Электрон. текстовые дан. – Москва : ФИЗМАТЛИТ, 2013. – 280 с	<a href="http://www.iprbbookshop.ru/24451">http://www.iprbbookshop.ru/24451</a>	
<b>ДОПОЛНИТЕЛЬНАЯ</b>						
4.	Лк, лб, ср	Основы информационной безопасности	Расторгуев С.П.	М.: Интернет-Университет Информационных Технологий (ИНГУИТ), 2016. — 590 с. — 5-9556-0067-1.	<a href="http://www.iprbbookshop.ru/73733.html">http://www.iprbbookshop.ru/73733.html</a>	
5.	Лк, лб, ср	Организационная защита информации	Рытов М.Ю.	МГТУ, 2015. – 486 с.	<a href="http://znanium.com/bookread.php?book=405000">http://znanium.com/bookread.php?book=405000</a>	
<b>ИНТЕРНЕТ - РЕСУРСЫ</b>						
6.	Лк, пз, лб, ср	<a href="http://www.interface.ru">http://www.interface.ru</a> - энциклопедия информационных технологий				
7.	Лк, пз, лб, ср	<a href="http://window.edu.ru">http://window.edu.ru</a> – единое окно доступа к образовательным ресурсам				
8.	Лк, пз, лб, ср	<a href="http://www.intuit.ru">http://www.intuit.ru</a> – интернет-университет				
9.	Лк, пз, лб, ср	<a href="http://www.e.lanbook.com/books">http://www.e.lanbook.com/books</a> – Электронно-библиотечная система				
10.	Лк, пз, лб, ср	<a href="http://www.twirpx.com">www.twirpx.com</a> ресурс для студентов и преподавателей				

## 7.2. Программное обеспечение

Интегрированные среды разработки программ Borland Developer Studio и Visual Studio . NET, базы данных, информационно – справочные и поисковые системы; вузовские электронно-библиотечные системы учебной литературы.

## 8. Материально-техническое обеспечение дисциплины

Для проведения лекционных занятий на факультете имеется комплект технических средств обучения в составе:

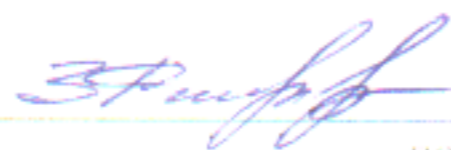
- интерактивная доска;
- переносной компьютер (в конфигурации не хуже: процессор IntelCore 2 Duo, 2 Гбайта ОЗУ, 500 Гбайт НЖМД);
- проектор (разрешение не менее 1280x1024);

Для проведения лабораторных занятий имеется компьютерный класс, оборудованный компьютерами с установленным программным обеспечением, предусмотренным программой дисциплины.

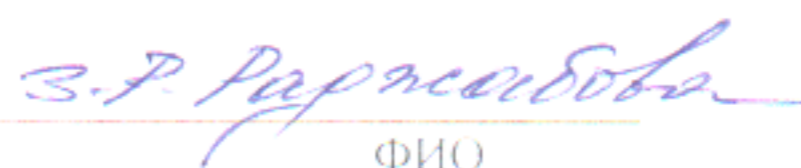
Программа составлена в соответствии с требованиями ФГОС ВО по направлению 10.03.01 – «Информационная безопасность», профиль «Безопасность автоматизированных систем».

Рецензент от выпускающей кафедры по направлению 10.03.01 Информационная безопасность

по направлению



подпись.



ФИО