Федеральное государственное бюджетное образовательное учреждение высшего образования
«Калининградский государственный технический университет»
Балтийская государственная академия рыбопромыслового флота
ФГБОУ ВО «КГТУ»
БГАРФ

УТВЕРЖДАЮ
Декан РТФ
_____ В.А. Баженов
27 июня 2018 г.

РАБОЧАЯ ПРОГРАММАДИСЦИПЛИНЫ

«Технология построения защищенных распределенных приложений»

(наименование дисциплины)

базовой части образовательной программы по специальности

10.05.03 «Информационная безопасность автоматизированных систем»
(код и наименование)

Специализация

Обеспечение информационной безопасности распределенных информационных систем
(наименование)

Факультет – **РАДИОТЕХНИЧЕСКИЙ (РТФ)**

Кафедра – **«ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»**

Калининград 2018

1.Цель освоения дисциплины.

1.1. Цели дисциплины

Учебная дисциплина «Технология построения защищенных распределенных приложений» обеспечивает приобретение знаний у студентов в области разработки распределенных приложений с использованием технологии Microsoft .NET.

Формирование у студентов понятий о современных подходах к проектированию и построению, эксплуатации и модернизации защищенного программного обеспечения.Формирование у студентов системных представлений о каноническом, автоматизированном, типовом подходе к проектированию распределенного программного обеспечения с применением современных CASE-средств, методов тестирования программного обеспечения, методов защиты программного обеспечения.

Формирование у студентов практических навыков использования CASE-средств для построения и модернизации программного обеспечения.

1.2. Задачи дисциплины

- изучение базовых требований к технологии построения защищенных распределенных приложений;
- изучение стандартов и архитектур защищенных распределенных приложений;
- изучение языка программирования C#;
- изучение технологииWindowsCommunicationFoundation;
- изучение принципов построения распределенных систем и объектно-ориентированных систем управления базами данных;
- формирование умений по применению принципов построения защищенных распределенных приложений;
-использование сетевой инфраструктуры для распределенной обработки и хранения данных;
- разработка алгоритмов и методов решения прикладных задач в распределенных вычислительных средах;
- изучение способов обеспечения безопасности на различных уровнях при разработке распределенных приложения.

1.3 Объекты предмета изучения дисциплины:

- принципы построения распределенных систем и обьектно-ориентированных систем управления базами данных;
- CASE– технологии для проектирования баз данных и хранилищ данных;
- требования к архитектуре информационных систем и их компонентам для обеспечения безопасности функционирования;
- нормативные документы по метрологии, стандартизации и сертификации программных и аппаратных средств защиты.

2. Результаты освоения дисциплины

Таблица 1 - Компетенции, формируемые в результате освоения дисциплины

Компетенции выпускника ОП ВО и этапы их формирования в результате изучения дисциплины	Этапы формирования компетенции		Знания, умения и навыки, характеризующие этапы формирования компетенций
1			2
ОПК-4.1способностью понимать значение информации в развитии современного общества, применять достижения современных информационных технологий для поиска информациив компьютерных системах, сетях, библиотечных фондах	**Знать:**		**Знать:** Основные способы создания защищенных распределенных приложений **Уметь** Использовать знания о принципах построения защищенных приложений, применять знания на практике **Владеть** основными методами научного познания
	Уровень 1	типовые структуры и принципы организации компьютерных сетей;	
	Уровень 2	общие принципы построения и использования современных языков программирования высокого уровня; современные технологии и методы программирования;	
	Уровень 3	классификацию современных компьютерных систем.	
	Уметь		
	Уровень 1	пользоваться сетевыми средствами для обмена данными, в том числе с использованием глобальной информационной сети Интернет;	
	Уровень 2	работать с интегрированной средой разработки программного обеспечения; формировать требования и разрабатывать внешние спецификации для разрабатываемого программного обеспечения;разрабатывать прикладные программы, осуществляющие взаимодействие с базами данных;	
	Уровень 3	проектировать и администрировать компьютерные сети, реализовывать политику безопасности компьютерной сети;разрабатывать и администрировать базы данных и интерфейсы прикладных программ к базам данных;применять средства обеспечения безопасности данных.	
	Владеть		
	Уровень 1	методами теоретического исследования физических явлений и процессов;	
	Уровень 2	навыками эксплуатации и администрирования (в части, касающейся разграничения доступа, аутентификации и аудита) баз данных, локальных компьютерных сетей, программных систем с учетом требований по обеспечению информационной безопасности;	
	Уровень 3	навыками использования ЭВМ в анализе простейших шифров; навыками математического моделирования в криптографии.	

<table>
<tr><td rowspan="14">ПК-9.1: способностью участвовать в разработке защищенных автоматизированных систем в сфере профессиональной деятельности</td><td colspan="2">Знать:</td><td rowspan="14">Знать:
Основные средства и способы обеспечения информационной безопасности и принципы построения систем защиты информации

Уметь:
реализовывать политику безопасности баз данных и проводить выбор программно-аппаратных средств с целью обеспечения требуемого уровня защищенности

Владеть:
навыками использования программно-аппаратных средств обеспечения информационной безопасности автоматизированных систем</td></tr>
<tr><td>Уровень 1</td><td>физические явления и эффекты, используемые при обеспечении информационной безопасности автоматизированных систем;
язык программирования высокого уровня (объектно-ориентированное программирование);</td></tr>
<tr><td>Уровень 2</td><td>основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации;</td></tr>
<tr><td>Уровень 3</td><td>автоматизированную систему как объект информационного воздействия, критерии оценки ее защищенности и методы обеспечения ее информационной безопасности;
основные меры по защите информации в автоматизированных системах (организационные, правовые, программно-аппаратные, криптографические, технические).</td></tr>
<tr><td colspan="2">Уметь</td></tr>
<tr><td>Уровень 1</td><td>анализировать и применять физические явления и эффекты для решения практических задач обеспечения информационной безопасности;</td></tr>
<tr><td>Уровень 2</td><td>реализовывать политику безопасности баз данных;</td></tr>
<tr><td>Уровень 3</td><td>проводить выбор программно-аппаратных средств обеспечения информационной безопасности для использования их в составе автоматизированной системы с целью обеспечения требуемого уровня защищенности автоматизированной системы.</td></tr>
<tr><td colspan="2">Владеть</td></tr>
<tr><td>Уровень 1</td><td>навыками применения математического аппарата для решения прикладных теоретико-информационных задач;</td></tr>
<tr><td>Уровень 2</td><td>методами и средствами технической защиты информации;</td></tr>
<tr><td>Уровень 3</td><td>навыками использования программно-аппаратных средств обеспечения информационной безопасности автоматизированных систем;
методами теоретического исследования физических явлений и процессов.</td></tr>
<tr><td rowspan="3">ПК-20.1: способностью организовать разработку, внедрение, эксплуатацию и сопровождение автоматизированной системы с учетом требований информационной безопасности</td><td colspan="2">Знать:</td><td rowspan="3">Знать:принципы построения распределенных систем и объектно-ориентированных систем управления базами данных

Уметь: разрабатывать и администрировать базы данных и интерфейсы прикладных программ к базам данных</td></tr>
<tr><td>Уровень 1</td><td>принципы построения распределенных систем и объектно-ориентированных систем управления базами данных, технологии автоматизированного проектирования баз данных и хранилищ данных;</td></tr>
<tr><td>Уровень 2</td><td>требования к архитектуре информационных систем и их компонентам для обеспечения безопасности функционирования;</td></tr>
</table>

	Уровень 3	методы, обеспечивающие безопасность клиент-серверных приложений в WCF.	**Владеть:** методами снижения угроз безопасности информационных систем, вызванных ошибками на этапе проектирования, разработки и внедрения
	Уметь		
	Уровень 1	разрабатывать и администрировать базы данных и интерфейсы прикладных программ к базам данных;	
	Уровень 2	использовать технологии автоматизированного проектирования и структурный подход при проектировании информационных систем;	
	Уровень 3	определять ресурсы, необходимые для обеспечения безопасности информационной системы, использовать методы и средства определения технологической безопасности функционирования распределенной информационной системы.	
	Владеть		
	Уровень 1	навыками семантического моделирования данных, навыками проектирования информационных систем на базе корпоративных систем управления базами данных;	
	Уровень 2	методами снижения угроз безопасности информационных систем, вызванных ошибками на этапе проектирования, разработки и внедрения;	
	Уровень 3	методами, обеспечивающими безопасность распределенных приложений в WCF.	
ПСК-7.1.3: способностью разрабатывать и исследовать модели информационно-технологических ресурсов, разрабатывать модели угроз и модели нарушителя информационной безопасности в распределенных информационных системах	**Знать:**		**Знать:** Критерии оценки эффективности средств защиты, основные средства и способы обеспечения информационной безопасности в распределенных информационных системах **Уметь:** разрабатывать модели угроз нарушителя информационной безопасности и реализовывать политику безопасности баз данных **Владеть:** навыками разработки, эксплуатации и анализа политики безопасности распределенных информационных систем
	Уровень 1	критерии оценки эффективности и надежности средств защиты операционных систем; средства обеспечения безопасности данных;	
	Уровень 2	основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации;	
	Уровень 3	основные задачи и понятия криптографии; модели шифров и математические методы их исследования; методы обеспечения информационной безопасностиавтоматизированной системы; методы аттестации уровня защищенности автоматизированных систем.	
	Уметь		
	Уровень 1	оценивать эффективность и надежность защиты операционных систем;	
	Уровень 2	реализовывать политику безопасности баз данных; применять средства обеспечения безопасности данных;	
	Уровень 3	определять информационную инфраструктуру и информаци-	

		онные ресурсы организации, подлежащие защите.	
	Владеть		
	Уровень 1	навыками эксплуатации и администрирования программных систем с учетом требований по обеспечению информационной безопасности;	
	Уровень 2	навыками разработки, документирования баз данных с учетом требований по обеспечению информационной безопасности;	
	Уровень 3	навыками анализа и синтеза структурных и функциональных схем защищенных автоматизированных информационных систем.	

3. Место дисциплины в структуре образовательной программы

Дисциплина Б1.Б.36«Технология построения защищенных распределенных приложений» относится к базовой части профессионального цикла дисциплин специализации. Изучение базируется на следующих дисциплинах: «Языки программирования», «Информатика», «Дискретная математика», «Структуры и алгоритмы компьютерной обработки информации», «Организация ЭВМ и вычислительных сетей», «Сети и системы передачи информации», «Технологии и методы программирования».

Дисциплина необходима для освоения учебной практики, обучающиеся должны обладать знаниями, умениями и навыками, полученными в результате формирования и развития соответствующих компетенций.

4. Содержание дисциплины

Индекс, наименование дисциплины	Содержание дисциплины (дидактические единицы)	Всего часов
Б1.Б.36	Основы проектирования защищенных распределённых приложений. Распределенные базы данных как ядро распределенного приложения. Методы отладки защищенных распределенных приложений. Ввод в эксплуатацию защищенного распределенного приложения. Способы обеспечения безопасности при создании распределенных приложений.	216

Раздел 1.**WindowsCommunicationFoundation (WCF) – современная технология построения защищенных распределенных систем.**
Тема 1.1.Основные понятияWCF.Базовая композиция приложения WCF. Понятие ABCWCF. Контракты. Привязки. Адреса.
Тема 1.2. Язык определения XML-схемы
Тема 1.3 Протокол SOAP
РАЗДЕЛ 2. **Контракты.**
Тема 2.1Контракты служб. Контракты ошибок
Тема 2.2. VisualStudio. C#.Создание контракта службы
Тема 2.3. Контракты данных. Коллекции.Контрактысообщений.Сериализация
Тема 2.4 Определение и использование расширяемого контракта данных
РАЗДЕЛ 3. **Экспонирование служб.**
Тема 3.1. Суть конечных точек службы. Создание конечных точек с помощью файла конфигурации. Базовые адреса
Тема 3.2. Общие сведения об архитектуре метаданных
Тема 3.3. Настройка стандартных привязок. Нестандартные привязки
РАЗДЕЛ 4. **Создание в WCFработающих с базами данныхклиент-серверных приложений**
Тема 4.1. Работа с базой данных Accessв C#./Тема 4.2. Классификация уязвимостей информационных систем.
РАЗДЕЛ 5. **Использование служб.**
Тема 5.1. Использование утилиты svcutilдля генерирования прокси-класса
Тема 5.2. Использование среды VisualStudioдля генерирования прокси-класса
Тема 5.3 Определение прокси-класса вручную.
Тема 5.4 Использование прокси для вызова служб. Динамическое создание прокси-класса
РАЗДЕЛ 6. **Настройка WCF.**
Тема 6.1. Конфигурирование конечной точки клиента
РАЗДЕЛ 7. **Средства контроля.**

Тема 7.1 Базовая трассировка в WCF

РАЗДЕЛ 8. **Инфраструктура безопасности**

Тема 8.1Обеспечение безопасности на транспортном уровне. Привязки и безопасность. Обеспечение безопасности на уровне сообщений

Тема 8.2 Основы проверки подлинности.Политика безопасности. Учетные данные клиентов. Учетные данные службы. Собственная проверка подлинности

Тема 8.3 Авторизация и персонификация. Авторизация на основе заявок. Проверка подлинности с помощью маркеров безопасности. Персонификация

РАЗДЕЛ 9. **Обработка транзакций.**

Тема 9.1 Свойства транзакций. Реализация ACID. Протоколы транзакций. Распространение транзакций. Транзакции и однонаправленные вызовы

5. Объем (трудоемкость освоения) и структура дисциплины, формы аттестации по ней

Таблица 2 - Структура дисциплины по очной форме обучения

Номер и наименование раздела, темы	Объем учебной работы (час.)				
	Лекции	ЛЗ	ПЗ	СРС	Всего
Семестр – 8 (4 ЗЕТ, 216 час.)					
РАЗДЕЛ 1. WindowsCommunicationFoundation (WCF) – современная технология построения защищенных распределенных систем.	**4**	**8**	**-**	**10**	**22**
Тема 1.1. Основные понятия WCF.Базовая композиция приложения WCF. Понятие ABC WCF. Контракты. Привязки. Адреса.	2	-	-	6	8
Тема 1.2. Язык определения XML-схемы	1	4	-	2	6
Тема 1.3 Протокол SOAP	1	4		2	
РАЗДЕЛ 2. Контракты	**6**	**6**	**-**	**14**	**26**
Тема 2.1. Контракты служб. Контракты ошибок	2	-	-	6	10
Тема 2.2. VisualStudio. C#.Создание контракта службы	2	4	-	2	12
Тема 2.3. Контракты данных. Коллекции.Контрактысообщений.Сериализация	2	1	-	2	
Тема 2.4 Определение и использование расширяемого контракта данных	2	1	-	4	
РАЗДЕЛ 3. Экспонирование служб	**4**	**8**	**-**	**12**	**24**
Тема 3.1. Суть конечных точек службы. Создание конечных точек с помощью файла конфигурации. Базовые адреса	2	-	-	6	10
Тема 3.2. Общие сведения об архитектуре метаданных	1	4	-	4	8
Тема 3.3. Настройка стандартных привязок. Нестандартные привязки	1	4	-	2	
РАЗДЕЛ 4. Создание в WCF работающих с базами данных клиент-серверных приложений	**2**	**10**	**-**	**10**	**22**
Тема 4.1. Работа с базой данных Accessв C#./Тема 4.2. Классификация уязвимостей информационных систем	2	10	-	10	10
РАЗДЕЛ 5. Использование служб	**6**	**12**	**-**	**12**	**30**
Тема 5.1. Использование утилиты svcutil для генерирования прокси-класса	1	4	-	4	6
Тема 5.2. Использование среды VisualStudioдля генерирования прокси-класса	1	4	-	4	8
Тема 5.3 Определение прокси-класса вручную	2	2	-	2	16

Тема 5.4 Использование прокси для вызова служб. Динамическое создание прокси-класса	2	2	-	4	4
РАЗДЕЛ 6. Настройка WCF	**2**	**8**	**-**	**8**	**18**
Тема 6.1. Конфигурирование конечной точки клиента	2	8	-	8	26
РАЗДЕЛ 7. Средства контроля	**2**	**2**	**-**	**8**	**12**
Тема 7.1 Базовая трассировка в WCF	2	2	-	8	16
РАЗДЕЛ 8. Инфраструктура безопасности	**6**	**12**	**-**	**10**	**28**
Тема 8.1Обеспечение безопасности на транспортном уровне. Привязки и безопасность. Обеспечение безопасности на уровне сообщений	2	4	-	2	
Тема 8.2 Основы проверки подлинности.Политика безопасности. Учетные данные клиентов. Учетные данные службы. Собственная проверка подлинности	2	4	-	4	
Тема 8.3 Авторизация и персонификация. Авторизация на основе заявок. Проверка подлинности с помощью маркеров безопасности. Персонификация	2	4	-	4	
РАЗДЕЛ 9. Обработка транзакций	**2**	**2**	**-**	**3**	**7**
Тема 9.1 Свойства транзакций. Реализация ACID. Протоколы транзакций. Распространение транзакций. Транзакции и однонаправленные вызовы	2	2	-	3	
Подготовка к сдаче и сдача экзамена				**27**	**27**
Итого по дисциплине	**34**	**68**	**-**	**87**	**216**
	102				

ЛЗ – лабораторные занятия,
ПЗ – практические занятия,
СРС – самостоятельная работа студента

6. Лабораторные занятия (работы)

Таблица 3 - Лабораторные занятия по очной форме обучения

№ ПЗ	Тема дисциплины	Тема и содержание ПЗ	Количествочасов ЛЗ
Семестр – 8 (68 час.).			
1.	Тема 1.1.	Определение основных особенностей построения распределенных приложений типа клиент-сервер	4
2.	Тема 1.1.	Настройка стандартных привязок	2
3.	Тема 1.1.	Настройка нестандартных привязок	2
4.	Тема 2.2.	СозданиебазовогоприложенияWindowsCommunicationFoundation – определение контракта службы	2
5.	Тема 2.2.	СозданиебазовогоприложенияWindowsCommunicationFoundation – реализация контракта службы	4
6.	Тема 2.3.	СозданиебазовогоприложенияWindowsCommunicationFoundation – создание клиента	4
7.	Тема 2.3.	СозданиебазовогоприложенияWindowsCommunicationFoundation – настройка клиента	2
8.	Тема 2.3.	СозданиебазовогоприложенияWindowsCommunicationFoundation – использование клиента	4

9.	Тема 3.1.	Созданиев конфигурационном файле трех конечных точек, использующих базовые адреса	4
10.	Тема 3.2.	Создание в коде трех конечных точек, использующих базовые адреса. Публикация метаданных посредством конечных точек	4
11.	Тема 3.3	Одна служба, несколько клиентов	2
12.	Тема 4.1	Простое консольное клиент-серверное приложение, выводящее информацию из базы данных Access	4
13.	Тема 4.1	В приложении клиентаWindowsForms: вывод информации, полученной от сервера, в DataGridView. В консольном приложении сервера: получение информации из базы данныхAccess и передача ее клиенту	4
14.	Тема 4.1	WindowsForms приложение клиента, выводящее информацию, полученную от сервера, в DataGridViewна форме. Получение информации из базы данных SQLServer 2005 и передача ее клиенту в консольном приложении сервера	6
15.	Тема 5.1	Создание прокси-класса с помощью утилиты svcutil. Создание ссылки на службу средствами VisualStudio. Сравнительная характеристика этих двух методов генерирования прокси-класса	4
16.	Тема 5.3.	Создание прокси-класса вручную	2
17.	Тема 5.	Динамическое создание прокси-класса	2
18.	Тема 6.1	Конфигурирование конечной точки клиена	4
19.	Тема 8.1.	Транспортная безопасность в привязках, основанных на TCP	2
20.	Тема 8.2	Транспортная безопасность в привязке, основанной на HTTP	2
21.	Тема 8.3.	Конфигурирование базовой безопасности сообщений	2
22.	Тема 8.3.	Использование сертификатов для проверки подлинности.	2
23.	Тема 9.1	Создание службы, позволяющей поток транзакций	2
Всего за семестр:			68
Итого по дисциплине			**68**

7. Практические занятия

Практические занятия по дисциплине учебным планом не предусмотрены.

8.Самостоятельная работа студента

Таблица 4 - Самостоятельная работа студента по очной форме обучения

№	Вид (содержание) СРС	Количество часов СРС	Форма контроля,аттестации
Семестр – 4			
1.	История развития систем защиты информации в зарубежных странах	6	конспект лекций, реферат
2.	Информационное противоборство в системе международных отношений современного общества	6	конспект лекций
3.	Стандарты информационной безопасности	6	конспект лекций

4.	Виды защищаемой информации.	6	конспект лекций
5.	Правонарушения в области обеспечения информационной безопасности.	6	конспект лекций, реферат
6.	Правовые режимы защиты информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну	6	конспект лекций
7.	Правовой режим обеспечения безопасности персональных данных	6	конспект лекций
8.	Система управления (менеджмента) информационной безопасности	6	конспект лекций
Всего за семестр:		**87**	
Итого по дисциплине		**87**	

9. Учебная литература и учебно-методическое обеспечение самостоятельной работы студента

9.1. Основная учебная литература

1. Мельников, В. П. Информационная безопасность и защита информации: учеб.пособие для вузов / В. П. Мельников, С. А. Клейменов, А. М. Петраков; ред. С. А. Клейменов. – Москва: Академия, 2008. – 330 с.(наличие в библиотеке БГАРФ - 31 экз.)

9.2. Дополнительнаяучебнаялитература

1. Троелсен, Э.

Язык программирования C# 2008 и платформа .NET 3.5 [Текст] : практическое пособие; пер. с англ. / Э. Троелсен. - 4-е изд. - М. ; СПб. ; Киев : ИД "Вильямс", 2011. - 1344 с. : ил

(2 экз.)

10. Информационные технологии, программное обеспечение и Интернет-ресурсы дисциплины.

Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем:

ЭБС «БГАРФ» **http://bgarf.ru/academy/biblioteka/**
ЭБС «КГТУ» **http://www.klgtu.ru/library/**
Университетская библиотека Online(г. Москва)**https://biblioclub.ru/**
«Кодекс»/«Техэксперт»**https://kodeks.ru/**
Редакция базы данных POLPRED.COMhttps://polpred.com/
Научная лицензионная библиотека eLIBRARY.RU https://elibrary.ru/defaultx.asp
ЭБС "IPRbooks" **http://www.iprbookshop.ru/**

ЭБС "Лань" **https://e.lanbook.com/**

ЭБС Издательского центра «Академия» http://www.academia-moscow.ru/elibrary

Материально-техническое обеспечение дисциплины

11.1. Общие требования к материально-техническому обеспечению дисциплины

11.1.1. Материально-техническое обеспечение для лекционных занятий

Для проведения лекционных занятий используется ауд.441.

Состав оборудования: учебная мебель; экран раздвижной - 1 шт.; доска маркерная - 1 шт.; мультимедийный проектор TOSHIBA – 1шт.; ноутбук AcerExtensa – 1 шт.

Используется лицензионное программное обеспечение MicrosoftWindows 10, Microsoft-Office 2016, Kaspersky EndpointSecurity 10 дляWindows.

11.1.2. Материально-техническое обеспечение для лабораторных занятий

Для проведения лабораторных занятий используется:

состав оборудования: учебная мебель; доска маркерная - 1 шт.; мультимедийный проектор TOSHIBA – 1шт.; ноутбук AcerExtensa – 1 шт.;

Для проведения лабораторных занятий используются ауд.248, 250:

Состав оборудования: учебная мебель; доска маркерная - 2 шт.; персональные ЭВМ, объединенные в локальную вычислительную сеть Internet – 27 шт., мультимедийный проектор TOSHIBA – 1шт.; ноутбук AcerExtensa – 1 шт.

Используется лицензионное программное обеспечение Операционные системы: Microsoft Windows Desktop operating systems, офисные приложения: Microsoft Office, по соглашению V9002148 Open Value Subscription, Kaspersky Total Space Security Russian Edition.

Программное обеспечение, распространяемое по лицензии GNU General Public License (лицензия на свободное программное обеспечение, созданная в рамках проекта GNU, по которой автор передает программное обеспечение в общественную собственность).

11.1.3. Материально-техническое обеспечение для самостоятельной работы

Для самостоятельной работы используется компьютерные классы.

Для проведения лабораторных занятий используются ауд. 248,250:

Состав оборудования: учебная мебель; доска маркерная - 2 шт.; персональные ЭВМ, объединенные в локальную вычислительную сеть Internet – 27 шт.; мультимедийный проектор TOSHIBA – 1шт.; ноутбук AcerExtensa – 1 шт.

Используется лицензионное программное обеспечение Операционные системы: Microsoft Windows Desktop operating systems, офисные приложения: Microsoft Office, по соглашению V9002148 Open Value Subscription, Kaspersky Total Space Security Russian Edition.

Программное обеспечение, распространяемое по лицензии GNU General Public License (лицензия на свободное программное обеспечение, созданная в рамках проекта GNU, по которой автор передает программное обеспечение в общественную собственность).

11.2. Материально-техническое обеспечение дисциплины для лиц с ограниченными возможностями здоровья

Освоение дисциплины лицами с ОВЗ осуществляется с использованием средств обучения общего и специального назначения.

При обучении студентов с нарушениями слуха предусмотрено использование звукоусиливающей аппаратуры, мультимедийных средств и других технических средств приема/передачи учебной информации в доступных формах для студентов с нарушениями слуха, мобильной системы обучения для студентов с инвалидностью, портативной индукционной системы. Учебная аудитория, в которой обучаются студенты с нарушением слуха, оборудована компьютерной техникой,аудиотехникой, видеотехникой, электронной доской, мультимедийной системой.

При обучении студентов с нарушениями зрениями предусмотрено использование в лекционных и учебных аудиториях возможности просмотра удаленных объектов (например, текста надоске или слайда на экране) при помощи видеоувеличителей для удаленного просмотра.

При обучении студентов с нарушениями опорно-двигательного аппарата используются альтернативные устройства ввода информации и другие технические средства приема/передачи учебной информации в доступных формах для студентов с нарушениями опорно-двигательного аппарата, мобильной системы обучения для людей с инвалидностью.

11. Фонд оценочных средств для проведения аттестации по дисциплине

Аттестация по дисциплине (итоговая аттестация по дисциплине является промежуточной аттестацией по образовательной программе). Для рабочей программы разработано и утверждено приложение «Фонд оценочных средств» для аттестации по дисциплине «Технология построения защищенных распределенных приложений».

12. Особенности преподавания и освоения дисциплины

В ходе изучения дисциплины предусматривается применение эффективных методик обучения, которые предполагают постановку вопросов проблемного характера с разрешением их, как непосредственно в ходе занятий, так и в ходе самостоятельной работы.Реализация программы предполагает использование интерактивных форм проведения лабораторных занятий. Проведение лабораторных занятий подразумевает обучение, построенное на групповой совместной деятельности студентов, в том числе с использованием персонального компьютера.

Перед началом занятий преподаватель проводит инструктаж по технике электробезопасности и пожарной безопасности.Контроль знаний в ходе изучения дисциплины осуществляется в виде текущих контролей, а также итоговой аттестации в форме дифференцированного зачета по итогам учебного семестра.

Текущие контроли предназначены для проверки хода и качества усвоения обучающимися учебного материала и стимулирования учебной работы студентов. Они могут осуществляться в ходе всех видов занятий в форме, избранной преподавателем или предусмотренной рабочей программой дисциплины.Текущие контроли предполагают постоянный контроль преподавателем качества усвоения учебного материала, активизацию учебной деятельности студентов на занятиях, побуждение их к самостоятельной систематической работе. Он необходим обучающимся для самоконтроля на разных этапах обучения. Их результаты учитываются выставлением оценок в журнале учета успеваемости.

К экзамену допускаются студенты, имеющие по всем текущим контролям положительные оценки.

13. Методические указания по освоению дисциплины

Планирование и организация времени, необходимого на изучение дисциплины, предусматривается ФГОС ВОпо специальности 10.05.03 «Информационная безопасность автоматизированных систем» и рабочим учебным планом подготовки специалистов. Объем часов и формы работы по изучению дисциплины распределены в рабочей программе соответствующей дисциплины.

14.1 Общие сведения о дисциплине

Цель дисциплины «Технология построения защищенных распределенных приложений» — заложить терминологический фундамент, научить студентов разрабатывать распределенные приложения с использованием технологии Microsoft .NET., сформировать у студентов понятия о современных подходах к проектированию и построению, эксплуатации и модернизации защищенного программного обеспечения, формирование у студентов системных представлений о каноническом, автоматизированном, типовом подходе к проектированию распределенного программного обеспечения с применением современных CASE-средств, методов тестирования программного обеспечения, методов защиты программного обеспечения.

14.2. Виды занятий и способы контроля

В соответствии с рабочим учебным планом дисциплина «Технология построения защищенных распределенных приложений» включает следующие виды занятий: лекции, лабораторные занятия, самостоятельная работа студентов.

На лекциях излагаются основные теоретические положения, составляющие дисциплину, и разбираются примеры практических задач. Преподавателю, ведущему курс, рекомендуется на вводной лекции определить структуру курса, пояснить цели и задачи изучения дисциплины, сформулировать основные вопросы и требования к результатам освоения.

При рассмотрении темы важно выделить основные понятия и определения, желательна их визуализация. При подготовке и проведении занятий по данному курсу преподаватель должен руководствоваться как общими учебно-методическими принципами (научность, системность, доступность, последовательность, преемственность, наличие единой внутренней логики курса, его связь с другими предметами), так и специфическими особенностями дисциплины, которые находят выражение в агрегированности и комбинации подходов. В подборе материала к занятиям следует руководствоваться рабочей программой учебной дисциплины, обращая внимание на компетенции, указанные в федеральном государственном образовательном стандарте высшего образования.

На первом занятии преподаватель обязан довести до обучающихся порядок работы в

аудитории и нацелить их на проведение самостоятельной работы с учетом количества часов, отведенных на нее учебным планом. Рекомендуя литературу для самостоятельного изучения, преподаватель должен максимально использовать возможности, предлагаемые библиотекой академии, в том числе ее электронными ресурсами.

Во время лекционных занятий рекомендуется вести конспектирование учебного материала, обращать внимание на формулировки и категории, раскрывающие суть того или иного явления или процессов, научные выводы и практические рекомендации.

Проблемная лекция побуждает аудиторию к активному включению в усвоение и обсуждение материала. Нахождение ответов на неоднозначные вопросы стимулирует развитие творческого мышления. Вопросы, предлагаемые аудитории для размышления, должны побуждать обучаемых использовать имеющиеся знания.

В конце лекции необходимо делать выводы и ставить задачи на самостоятельную работу.

Практические занятия направлены на закрепление лекционного материала.

Самостоятельная работа студентов заключается в подготовке к практическим и лекционным занятиям и выполнении домашних заданий, выдаваемых преподавателем по каждому из разделов дисциплины. В целях лучшего понимания сути представления и обработки информации при защите рекомендуется использовать гипотетическую модель информации, что позволит использовать архитектурные особенности, свойственные конкретным моделям анализа. Примеры следует выбирать так, чтобы вычисления были не слишком громоздкими. Следует рассматривать задачи, возникающие в самых различных отраслях и показать динамику решения задач: как подойти к решению конкретной проблемы, какие ограничения возникают в рамках данного решения и какие результаты получаются в конечном счете.

В идеальном случае процесс обучения должен происходить следующим образом: студент слушает лекции, читает учебную литературу, работает дома и на практических занятиях. Студенту рекомендуется иметь доступ к компьютеру во время самостоятельной работы для выполнения индивидуальных заданий. Подготовка к каждой работе производится во внеаудиторное время.

В самостоятельную работу входит выполнение индивидуальных заданий. Преподаватель принимает решение о допуске студента к практической работе по результатам собеседования. Студенты знакомятся с общими сведениями, порядком выполнения работы, пишут необходимые пояснения в соответствии с полученным вариантом задания. При защите работы студент отвечает преподавателю на контрольные вопросы, представляет теоретическую часть решения задачи, практический расчет.

Правильная организация самостоятельных учебных занятий, их систематичность, целесообразное планирование рабочего времени позволяет привить студентам умения и навыки в овладении, изучении, усвоении и систематизации приобретаемых знаний в процессе обучения, обеспечивать высокий уровень успеваемости в период обучения, привить навыки повышения профессионального уровня в течение всей трудовой деятельности.

Рабочая программа дисциплины «Технология построения защищённых распределённых приложений» представляет собой компонент образовательной программы специалитета по специальности 10.05.03 «Информационная безопасность автоматизированных систем», специализации «Обеспечение информационной безопасности распределенных информационных систем» и соответствует учебному плану, утвержденному 31 января 2018 г. и действующему для студентов, принятых на первый курс, начиная с 2014 года.

Автор программы – ассистент кафедры «Информационная безопасность» Бабаева А.А.

Рабочая программа дисциплины рассмотрена и одобрена на заседании кафедры «Информационная безопасность»
(протокол № 9 от 14 июня 2018 г.)

Заведующий кафедрой _____ /Н.Я. Великите/

Рабочая программа дисциплины рассмотрена и одобрена на заседании методической комиссии Совета РТФ

(протокол № 6 от 27 июня 2018 г.)

Председатель методической комиссии _____ /А.Г. Жестовский/