

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«КАЛИНИНГРАДСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

А. А. Бабаева

ТЕХНОЛОГИЯ ПОСТРОЕНИЯ ЗАЩИЩЕННЫХ ПРИЛОЖЕНИЙ ДЛЯ ОТКРЫТЫХ СИСТЕМ

Учебно-методическое пособие по изучению дисциплины для студентов
специалитета по специальности 10.05.03 «Информационная безопасность
автоматизированных систем», специализация «Безопасность открытых
информационных систем»

Калининград
Издательство ФГБОУ ВО «КГТУ»
2025

УДК 004.056.57 (076)

Рецензент

кандидат физико-математических наук, доцент кафедры информационной безопасности ФГБОУ ВО «Калининградский государственный технический университет Н. Я. Великите

Бабаева, А. А.

Технология построения защищенных приложений для открытых систем: учебно-методическое пособие по изучению дисциплины для студентов специалитета по специальности 10.05.03 «Информационная безопасность автоматизированных систем», специализация «Безопасность открытых информационных систем»/ А. А. Бабаева. – Калининград: Изд-во ФГБОУ ВО «КГТУ», 2025. – 38 с.

Учебно-методическое пособие является руководством по изучению дисциплины «Технология построения защищенных приложений для открытых систем» студентами специалитета 10.05.03 «Информационная безопасность автоматизированных систем», специализация «Безопасность открытых информационных систем». В документе представлен тематический план изучения дисциплины, содержание дисциплины по ее разделам и темам, указания к изучению каждой темы, вопросы для изучения методических материалов к занятиям, методические указания по выполнению самостоятельной работы, содержатся требования к текущей и промежуточной аттестации.

Учебно-методическое пособие предназначено для изучения теоретического материала и приобретения навыков проектирования, создания, эксплуатации, приложений для открытых систем и обеспечения их безопасности на всех этапах жизненного цикла.

Табл. 2, список лит. – 14 наименования

Учебно-методическое пособие по изучению дисциплины рекомендовано к использованию в качестве локального электронного методического материала в учебном процессе методической комиссией ИЦТ 26.05.2025 г., протокол № 4

УДК 004.056.57 (076)

© Федеральное государственное бюджетное образовательное учреждение высшего образования «Калининградский государственный технический университет», 2025 г.
© Бабаева А. А., 2025 г.

ОГЛАВЛЕНИЕ

1. Введение.....	4
2. Тематический план.....	6
3. Содержание дисциплины и указания к изучению.....	10
4. Методические рекомендации по подготовке к лабораторным занятиям.....	24
5. Методические указания по самостоятельной работе	25
6. Требования к аттестации по дисциплине.....	28
7. Заключение.....	33
8. Список литературы.....	35

1. ВВЕДЕНИЕ

Данное учебно-методическое пособие предназначено для студентов специалитета 10.05.03 Информационная безопасность автоматизированных систем», специализация «Безопасность открытых информационных систем», изучающих дисциплину «Технология построения защищенных приложений для открытых систем».

ОПК-5.3. Способен осуществлять контроль обеспечения информационной безопасности и проводить верификацию данных в открытых информационных системах.

Цель освоения дисциплины: целостное представление о способах разработки распределенных приложений для открытых систем с использованием технологии Microsoft.NET, сформируют понятия о современных подходах к проектированию и построению, эксплуатации и модернизации защищенного программного обеспечения.

В результате освоения дисциплины обучающийся должен:

знать:

- нормативные документы по метрологии, стандартизации и сертификации программных и аппаратных средств защиты информации в открытых информационных системах;
- методы тестирования и отладки, принципы организации документирования разработки, процесса сопровождения программного обеспечения;

уметь:

- определять эффективность применения средств информатизации;

владеть:

- методами, способами и средствами обеспечения отказоустойчивости для открытых систем.

Задачи дисциплины:

- изучение базовых требований к технологии построения защищенных распределенных приложений для открытых систем;
- изучение стандартов и архитектур защищенных распределенных приложений для открытых систем;
- изучение языка программирования C#;
- изучение технологии Windows Communication Foundation;
- изучение принципов построения распределенных систем и объектно-ориентированных систем управления базами данных;
- формирование умений по применению принципов построения защищенных распределенных приложений для открытых систем;

- 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 приложений для открытых систем.

Дисциплина «Технология построения защищенных приложений для открытых систем» относится к Модулю «Дисциплины специализации» направления подготовки 10.05.03 Информационная безопасность автоматизированных систем.

Для выполнения лабораторных работ используется среда Visual Studio и язык программирования C#.

Основными видами аудиторных учебных занятий по дисциплине являются лекции и лабораторные занятия.

Формирование знаний, обучающихся обеспечивается проведением лекционных занятий.

Далее в пособии представлен тематический план, содержащий перечень изучаемых тем, обязательных лабораторных работ, мероприятий текущей аттестации и отводимое на них аудиторное время (занятия в соответствии с расписанием) и самостоятельную работу. При формировании личного образовательного плана на семестр следует оценивать рекомендуемое время на изучение дисциплины; возможно, вам потребуется больше времени на выполнение отдельных заданий или проработку отдельных тем.

В разделе «Содержание дисциплины» приведены подробные сведения об изучаемых вопросах, по которым вы можете ориентироваться в случае пропуска каких-то занятий, а также методические рекомендации преподавателя для самостоятельной подготовки, каждая тема имеет ссылки на литературу (или иные информационные ресурсы) и контрольные вопросы для самопроверки.

Раздел «Текущая аттестация» содержит описание обязательных мероприятий контроля самостоятельной работы и усвоения разделов или отдельных тем дисциплины. Далее изложены требования к завершающей аттестации – зачету и экзамену.

Помимо данного пособия, студентам следует использовать материалы, размещенные в соответствующем данной дисциплине разделе ЭИОС, в которые более оперативно вносятся изменения для адаптации дисциплины под конкретную группу.

2. ТЕМАТИЧЕСКИЙ ПЛАН

2.1. Очная форма обучения

Таблица 1

	Раздел (модуль) дисциплины	Тема	Объем контакт- ной работы, ч	Объем самос- тоятельной работы, ч
		Теоретическое обучение (лекции) Семестр 10, 11		
1	Основы распределенных вычислений для открытых систем	Тема 1.1: Парадигма распределённых вычислений Тема 2.2: Особенности создания распределенных приложений для открытых систем	2	2
2	Windows Communication Foundation (WCF) – современная технология построения защищенных распределенных систем	Тема 2.1: Основные понятия WCF. Тема 2.2: Язык определения XML-схемы Тема 2.3: Протокол SOAP	4	6
3	Контракты	Тема 3.1: Контракты служб. Контракты ошибок Тема 3.2: Visual Studio C#. Создание контракта службы Тема 3.3: Контракты данных. Коллекции. Контракты сообщений. Сериализация	5	6
4	Экспонирование служб	Тема 4.1: Суть конечных точек службы. Создание конечных точек с помощью файла конфигурации. Базовые адреса Тема 4.2: Общие сведения об архитектуре метаданных Тема 4.3: Настройка стандартных привязок. Нестандартные привязки	6	7
5	Создание в WCF служб, работающих с базами данных клиент-серверных приложений	Тема 5.1: Работа с базой данных Access в C#	2	2

	Раздел (модуль) дисциплины	Тема	Объем контакт- ной работы, ч	Объем самос- тоятельной работы, ч
	Использование служб	Тема 6.1: Использование утилиты svcutil для генерирования прокси-класса Тема 6.2: Использование среды Visual Studio для генерирования прокси-класса Тема 6.3: Определение прокси-класса вручную. Динамическое создание прокси-класса	5	6
	Настройка WCF	Тема 7.1: Конфигурирование конечной точки клиента Тема 7.2: Базовая трассировка в WCF	4	3
	Инфраструктура безопасности	Тема 8.1: Обеспечение 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 Тема 8.4: Свойства транзакций. Протоколы транзакций, Распространение транзакций. Транзакции и однонаправленные вызовы	8	8
			56	100
Практические (лабораторные занятия)				
	Windows Communication Foundation (WCF) – современная технология построения защищенных распределенных систем.	– Определение основных особенностей построения распределенных приложений типа клиент-сервер – Настройка стандартных привязок – Настройка нестандартных привязок	10	3

	Раздел (модуль) дисциплины	Тема	Объем контакт- ной работы, ч	Объем самос- тоятельной работы, ч
	Контракты	Создание базового приложения Windows Communication Foundation – определение контракта службы – реализация контракта службы – создание клиента – настройка клиента – использование клиента	16	8
	Экспонирование служб	– Создание в коде трех конечных точек, использующих базовые адреса. Публикация метаданных посредством конечных точек – Создание в конфигурационном файле трех конечных точек, использующих базовые адреса – Одна служба, несколько клиентов	6	2
	Создание в WCF служб, работающих с базами данных клиент-серверных приложений	– Простое консольное клиент-серверное приложение, выводящее информацию из базы данных Access – В приложении клиента Windows Forms: вывод информации, полученной от сервера, в DataGridView. В консольном приложении сервера: получение информации из базы данных Access и передача ее клиенту	8	2
	Использование служб	– Создание прокси-класса с помощью утилиты svcutil. – Создание ссылки на службу средствами Visual Studio. – Сравнительная характеристика этих двух методов генерирования прокси-класса – Создание прокси-класса вручную – Динамическое создание прокси-класса	10	1

	Раздел (модуль) дисциплины	Тема	Объем контакт- ной работы, ч	Объем самос- тоятельной работы, ч
	Инфраструктура безопасности	– Транспортная безопасность в привязках, основанных на TSP – Транспортная безопасность в привязке, основанной на HTTP – Конфигурирование базовой безопасности сообщений – Создание службы, позволяющей поток транзакций – Использование сертификатов для проверки подлинности	18	4
			72	46,85
		Рубежный (текущий) и итоговый контроль		
	Тестирование	РЭ – 13 , КА – 1,4		
	Итоговый контроль (экзамен)			34,75
				34,75
			141	183

ИТОГО: 324

3. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ И УКАЗАНИЯ К ИЗУЧЕНИЮ

3.1. РАЗДЕЛ 1 ОСНОВЫ РАСПРЕДЕЛЕННЫХ ВЫЧИСЛЕНИЙ ДЛЯ ОТКРЫТЫХ СИСТЕМ

3.1.1 Тема 1.1 Парадигма распределённых вычислений

Перечень изучаемых вопросов

Этапы развития технологии распределенных вычислений, особенности использования. Основные технологии построения распределенных систем и приложений.

Методические указания к изучению

Рассматриваются основные современные технологии построения распределенных приложений и особенности использования распределённых вычислений. Изучаются платформы для создания распределенных приложений. Предусмотрена лабораторная работа по теме: Определение основных особенностей построения распределенных приложений типа клиент-сервер.

Литература: [1, с. 58–96], [3, с. 12–18], [4, с. 23–29].

Контрольные вопросы

1. Особенности создания распределенных приложений и использования распределенных вычислений.
2. Этапы развития технологии распределенных вычислений.
3. Основные платформы для создания распределенных приложений.
4. Обзор технологий, отличных от WCF ориентированных.

3.1.2 Тема 1.2 Особенности создания распределенных приложений для открытых систем

Перечень изучаемых вопросов

Технологии создания приложений для открытых систем и особенности обеспечения безопасности в них. Сервисы, стандарты для построения распределённых вычислений и служб для открытых систем.

Методические указания к изучению

Рассматриваются основные способы проектирования и создания распределенных приложений для открытых систем. Особенности применения настроек безопасности для них. Раскрываются понятия масштабируемости, расширяемости, интероперабельности и высокой готовности открытых систем. Предусмотрена лабораторная работа по теме: Определение основных особенностей построения распределенных приложений типа клиент-сервер.

Литература: [1, с. 58–96], [2, с. 76–101], [4, с. 42–50].

Контрольные вопросы

1. Особенности создания распределенных приложений для открытых систем.
2. Настройка безопасности для приложений для открытых систем.
3. Раскрыть понятия масштабируемости и расширяемости открытых систем.

3.2. РАЗДЕЛ 2 WINDOWS COMMUNICATION FOUNDATION (WCF) – СОВРЕМЕННАЯ ТЕХНОЛОГИЯ ПОСТРОЕНИЯ ЗАЩИЩЕННЫХ РАСПРЕДЕЛЕННЫХ СИСТЕМ

3.2.1 Тема 2.1 Основные понятия WCF

Перечень изучаемых вопросов

Базовая композиция приложения WCF; понятия АПК (адрес, привязка, контракт) WCF; контракты; привязки; адреса.

Методические указания к изучению

Рассматриваются основные термины и определения технологии WCF. Особенности применения и создания распределенных приложений в среде WCF. Раскрываются понятия АПК (адрес, привязка, контракт) для конечных точек служб. Изучаются особенности использования привязок и контрактов при создании конечных точек и служб с распределенными вычислениями.

Windows Communication Foundation (WCF) – это технология Microsoft для создания распределенных приложений, которые взаимодействуют через сеть. Базовая композиция приложения WCF включает:

- **Сервис** – реализует бизнес-логику и предоставляет функциональность.
- **Хост** – среда, в которой запускается сервис (например, консольное приложение, IIS).
- **Клиент** – приложение, взаимодействующее с сервисом.

Основные понятия АПК (**Адрес, Привязка, Контракт**) в WCF:

- **Адрес (Address)** – уникальное местоположение сервиса в сети, например, URL.
- **Привязка (Binding)** – определяет, как клиент и сервис взаимодействуют, включая транспорт, протоколы и безопасность.
- **Контракт (Contract)** – описывает операции, доступные клиенту.

Типы контрактов в WCF:

- **Сервисный контракт** – описывает методы, доступные клиенту.
- **Контракт данных** – определяет структуру передаваемых данных.
- **Контракт ошибок** – задает возможные исключения.

Различные привязки (binding):

- **BasicHttpBinding** – простой и совместимый с веб-службами.
- **WSHttpBinding** – поддерживает безопасность и транзакции.
- **NetTcpBinding** – оптимизирован для связности в корпоративных сетях.

Адреса WCF указывают расположение сервиса и обычно включают:

- Протокол (http, net.tcp).
- Домен или IP-адрес.

Предусмотрена лабораторная работа по теме: определение основных особенностей построения распределенных приложений типа клиент-сервер.

Литература: [1, с. 140–201], [2, с. 236–287].

Контрольные вопросы

1. Особенности создания распределенных приложений и использования распределенных вычислений.
2. Реализация WCF-службы. Способы создания конечной точки службы.
3. Реализация службы в коде и с использованием файла конфигурации.
4. Понятие контракта и понятие привязки.

3.2.2 Тема 2.2 Язык определения XML-схемы

Перечень изучаемых вопросов: схемы данных, структура документа XML, описание элементов, область применения документов XML.

Методические указания к изучению

Рассматриваются особенности создания документов XML, область их применения и основные элементы с описанием атрибутов и моделей содержания. Изучается применение документов XML в создании служб с распределенными вычислениями.

XML (Extensible Markup Language) – это язык разметки, используемый для хранения и передачи структурированных данных.

Схемы данных в XML

XML предоставляет возможность создания **схем данных**, которые определяют структуру и правила для XML-документов. Основные схемы:

- **DTD (Document Type Definition)** – задает правила структуры XML-документа.
- **XML Schema (XSD)** – более мощный инструмент, поддерживающий типизацию данных и строгие ограничения.

Структура документа XML

Документ XML организован в виде древовидной структуры и включает:

- **Пролог** (<?xml version="1.0" encoding="UTF-8"?>) – указывает версию и кодировку.
- **Корневой элемент** – главный узел документа, содержащий остальные данные.
- **Дочерние элементы** – вложенные структуры, которые описывают данные.
- **Атрибуты** – дополнительные сведения внутри элементов.

Описание элементов XML

Каждый элемент XML имеет имя и может содержать:

- **Текстовое содержимое**
- **Вложенные элементы**
- **Атрибуты** (например: <user id="123">Mars</user>).

Область применения XML

XML широко используется в разных сферах:

- **Веб-сервисы** (SOAP, REST API).
- **Конфигурационные файлы** в программировании.
- **Хранение данных** (например, RSS-ленты).
- **Обмен данными** между приложениями.

Литература: [1, с. 78–126], [2, с. 66–121], [4, с. 32–40].

Контрольные вопросы

1. Область применения XML документов.
2. Особенности использования документов такого типа.
3. Основные элементы документов (атрибуты и модели содержания).
4. Типы данных.
5. Применение документов XML для создания служб WCF.

3.2.3. Тема 2.3 Протокол SOAP

Перечень изучаемых вопросов: протоколы WCF, протоколы обмена структурированными сообщениями, распределенная вычислительная среда, структура протокола SOAP, типы ошибок в протоколе.

Методические указания к изучению

Рассматриваются основные виды протоколов обмена структурированными сообщениями в распределенной вычислительной среде. Изучается протокол SOAP, его особенности, область применения, структура.

Windows Communication Foundation (WCF) поддерживает различные **протоколы**, обеспечивающие надежный обмен данными между клиентами и сервисами. Среди них:

- **SOAP (Simple Object Access Protocol)** – XML-основанный протокол, обеспечивающий строгую структурированность сообщений.
- **REST (Representational State Transfer)** – более легковесный подход, использующий HTTP-протокол.
- **TCP, MSMQ, Named Pipes** – для коммуникации в корпоративных средах.

Протоколы обмена структурированными сообщениями

Обмен сообщениями в WCF строится на основе:

- **SOAP** – обеспечивает четко определенный формат передачи.
- **JSON/XML** – упрощает взаимодействие REST API.
- **WS- (WS-Security, WS-ReliableMessaging, WS-AtomicTransaction)*** – расширяют функциональность WCF.

Распределенная вычислительная среда

WCF функционирует в **распределенной среде**, обеспечивая связь между независимыми компонентами через сеть. Это позволяет:

- Масштабировать приложения.
- Повышать отказоустойчивость.
- Реализовывать сервис-ориентированную архитектуру (SOA).

Структура протокола SOAP

SOAP-сообщение состоит из:

- **Envelope** – общий контейнер.
- **Header** – метаданные запроса.
- **Body** – содержимое передаваемых данных.
- **Fault** – описание ошибок, если они возникают.

Типы ошибок в протоколе

В SOAP определены **стандартные ошибки**:

- **VersionMismatch** – несовместимость версий SOAP.
- **MustUnderstand** – обязательный заголовок не обработан.
- **Client** – ошибка на стороне клиента (неверный запрос).
- **Server** – ошибка на стороне сервера.

Литература: [1, с. 58–96], [3, с. 34–50], [4, с. 2–20].

Контрольные вопросы

1. Виды протоколов обмена структурированными сообщениями.
2. Особенности протокола SOAP, область применения.
3. Типы ошибок и способы работы с исключениями.

3.3 Раздел 3. Контракты

3.3.1 Тема 3.1 Контракты служб. Контракты ошибок

Перечень изучаемых вопросов: понятие контракта WCF, виды контрактов (контракт сообщений, данных, служб), WSDL формат, синхронный операции запрос – ответ.

Методические указания к изучению:

Рассматривается понятие контракта для служб WCF и три основных вида контрактов. Изучается структура документов XML и формат языка WSDL для описания сетевых служб.

Литература: [1, с. 98–136], [2, с. 234–278], [4, с. 42–50].

Контрольные вопросы

1. Что такое контракт в общем смысле?
2. Какие контракты бывают в WCF и их особенности применения?
3. Способы описания контрактов.

4. Способы отображения одной системы на другую.
5. Элементы языка WSDL.

3.3.2 Тема 3.2 Visual Studio C#. Создание контракта службы

Перечень изучаемых вопросов: Среда Visual Studio и особенности языка C#, контракт службы и его реализация, создание контракта в коде и в файле конфигурации.

Методические указания к изучению: Рассматривается среда разработки Visual Studio и особенности создания приложений и служб на языке C#. Изучается создание контракта службы и его реализация с помощью кода и файла конфигурации. Рассматривается настройка контракта службы.

Литература: [1, с. 58–96], [2, с. 76–101], [4, с. 42–50].

Контрольные вопросы

1. Особенности языка C# в среде Visual Studio.
2. Понятие контракта службы.
3. Настройка и использование контракта службы.

3.3.3 Тема 3.3 Контракты данных. Коллекции. Контракты сообщений. Сериализация

Перечень изучаемых вопросов: особенности контрактов для данных, их использование, примеры. Понятие коллекций в WCF. Определение иерархий классов в контрактах. Понятие контрактов сообщений, работа с не типизированными сообщениями. Сериализация.

Методические указания к изучению

Рассматриваются понятия контрактов данных и сообщений. Особенности их использования и настройки, определения иерархий классов и работа с нетипичными данными и сообщениями. Изучаются понятия коллекций и сериализации в WCF.

Литература:[1, с. 140–201], [2, с. 236–287].

Контрольные вопросы

1. Особенность использования контракта данных.
2. Понятие контракта сообщений.
3. Понятие социализации.
4. Что такое коллекции в WCF.

3.4 Раздел 4. Экспонирование служб

3.4.1 Тема 4.1 Суть конечных точек службы

Перечень изучаемых вопросов: конечные точки службы, создание конечных точек с помощью кода и файлов конфигурации, использование базовых адресов.

Методические указания к изучению

Рассматривается понятие конечной точки службы, настройка адреса, привязки и контракта. Изучается настройка конечной точки с помощью кода и файлов конфигурации. Раскрывается понятие базовых адресов службы.

Литература: [1, с. 289–301], [2, с. 136–187].

Контрольные вопросы:

1. Конечная точка службы, способа задания адреса, привязки, контракта.
2. Задание параметров конечной точки в файле конфигурации.
3. Понятие базовых адресов.

3.4.2 Тема 4.2 Общие сведения об архитектуре метаданных

Перечень изучаемых вопросов: форматы метаданных, конечная точка обмена метаданными, импорт и экспорт метаданных, использование и извлечение метаданных.

Методические указания к изучению

Рассматриваются способы создания метаданных и конечных точек для их публикации. Изучаются основные форматы представления метаданных, используемые протоколы. Рассматриваются вопросы импорта и экспорта метаданных и их использование.

Литература: [1, с. 140–201], [2, с. 236–287], [3, с. 40–46], [4, с. 36–54].

Контрольные вопросы

1. Форматы метаданных.
2. Способы создания конечной точки обмена метаданными.
3. Как произвести импорт и экспорт метаданных.

3.4.3 Тема 4.3 Настройка стандартных привязок. Нестандартные привязки

Перечень изучаемых вопросов: понятие привязки, сравнительные характеристики стандартных привязок, их функциональные особенности. Выбор привязки под конкретный запрос и службу. Использование

нестандартных привязок, удаление и добавление элементов привязки. Создание пользовательских привязок.

Методические указания к изучению

Рассматривается необходимость создания пользовательских привязок, особенности их создания и применения. Условия для настройки элементов привязки, удаление и добавление новых элементов. Изучаются область применения привязок различного типа и настройки безопасности в них.

Привязка (Binding) в Windows Communication Foundation (WCF) – это набор настроек, определяющих, как клиент и сервис взаимодействуют. Она включает транспорт (HTTP, TCP), формат сообщений (XML, JSON) и механизмы безопасности.

Сравнение стандартных привязок и их особенности

Различные привязки WCF обладают уникальными возможностями:

1. BasicHttpBinding: Простая, совместима с веб-службами.
2. WSHttpBinding: Поддержка безопасности, транзакций.
3. NetTcpBinding: Оптимизирована для внутренних корпоративных систем.
4. **NetNamedPipeBinding:** Используется для взаимодействия в пределах одной машины.

Выбор привязки под запрос и службу:

- для веб-приложений → BasicHttpBinding, WSHttpBinding;
- для корпоративных решений → NetTcpBinding;
- для высоконагруженных очередей → MSMQBinding;
- для локальных взаимодействий → NetNamedPipeBinding.

Использование нестандартных привязок

При необходимости можно добавлять или удалять элементы привязки, например:

- включать или отключать шифрование;
- изменять тип сериализации данных;
- добавлять сжатие сообщений для оптимизации.

Создание пользовательских привязок

В WCF можно создать **собственную привязку**, комбинируя элементы: csharp;

```
CustomBinding binding = new CustomBinding();  
binding.Elements.Add(new TcpTransportBindingElement());  
binding.Elements.Add(new TextMessageEncodingBindingElement());
```

Такой подход позволяет гибко адаптировать работу службы под требования конкретного приложения.

Литература: [1, с. 58–96], [3, с. 12–18], [4, с. 23–29].

Контрольные вопросы

1. Для чего создаются пользовательские привязки?

2. Каким образом можно добавить или удалить элементы привязки?
3. Настройки безопасности для привязок.

3.5 Раздел 5. Создание в WCF служб, работающих с базами данных клиент серверных приложений

3.5.1 Тема 5.1 Работа с базой данных Access в C#

Перечень изучаемых вопросов: база данных и ее взаимодействие со службами WCF, настройка работы службы и базы данных, особенности использования и взаимодействия. Подключение базы данных, добавление новых данных, работа с фильтрами.

Методические указания к изучению

Рассматриваются вопросы взаимодействия баз данных со службами на языке C#. Изучаются способы подключения и настройки баз данных и служб.

Литература: [1, с. 68–96], [3, с. 22–28], [4, с. 33–39].

Контрольные вопросы

1. Как подключить базу данных к службе WCF?
2. Настройка взаимодействия и использование баз данных.
3. Особенности настройки безопасности при использовании такого типа распределенных вычислений.

3.6 Раздел 6. Использование служб

3.6.1 Тема 6.1 Использование утилиты svcutil для генерирования прокси класса

Перечень изучаемых вопросов: обращение к службам с использованием клиента, служебные программы метаданных, язык описания веб-служб, прокси-классы и их создание, способы создания прокси классов.

Методические указания к изучению

Рассматриваются вопросы создания прокси классов, особенности их использования. Изучается метод генерации прокси-класса с использованием утилиты svcutil.

Литература: [1, с. 158–186], [3, с. 42–48], [4, с. 33–49].

Контрольные вопросы

1. Что такое прокси-класс?
2. Какие бывают способы создания и генерации прокси-классов?
3. Для чего нужна утилита svcutil, и как ее использовать?

3.6.2 Тема 6.2 Использование среды Visual Studio для генерирования прокси класса

Перечень изучаемых вопросов: обращение к службам с использованием клиента, служебные программы метаданных, язык описания веб-служб, прокси-классы и их создание, способы создания прокси классов.

Методические указания к изучению

Рассматриваются вопросы создания прокси классов, особенности их использования. Изучается метод генерации прокси-класса, с использованием среды Visual Studio.

Литература: [1, с. 58–96], [3, с. 22–28], [4, с. 33–39].

Контрольные вопросы

1. Что такое прокси-класс?
2. Какие бывают способы создания и генерации прокси-классов?
3. Как с помощью среды Visual Studio сгенерировать прокси-класс?

3.6.3 Тема 6.3 Определение прокси-класса вручную. Динамическое создание прокси-класса

Перечень изучаемых вопросов: обращение к службам с использованием клиента, служебные программы метаданных, язык описания веб-служб, прокси-классы и их создание, способы создания прокси классов, создание прокси-классов вручную, динамическое создание.

Методические указания к изучению

Рассматриваются вопросы создания прокси классов, особенности их использования. Изучается метод создания прокси-классов вручную и динамическое генерирование прокси класса. Преимущества и недостатки данных методов.

Литература: [1, с. 140–201], [2, с. 236–287], [3, с. 40–46], [4, с. 36–54].

Контрольные вопросы

1. Что такое прокси-класс?
2. В чем отличие способов создания прокси-классов?
3. Как можно сгенерировать его вручную или динамически. Особенности, преимущества и недостатки?

3. 7 Раздел 7. Настройка WCF

3.7.1 Тема 7.1 Конфигурирование конечной точки клиента

Перечень изучаемых вопросов: адрес, привязка и контракт конечных точек, создание конечной точки метаданных, особенности назначения адресов при использовании нескольких конечных точек. Создание конечной точки в коде и с помощью файла конфигурации.

Методические указания к изучению

вопросы создания конечных точек в коде и в файле конфигурации, их настройка. Задание и выбор адреса, привязки и контракта для конечной точки. Конечные точки метаданных.

Литература: [2, с. 236–287], [3, с. 40–46].

Контрольные вопросы

1. Как можно задать адрес, привязку и контракт для конечной точки?
2. Какие виды конечных точек бывают?
3. Особенности конфигурирования конечной точки клиента.

3.7.2 Тема 7.2 Базовая трассировка в WCF

Перечень изучаемых вопросов: трассировка в WCF, виды трассировки, область применения и особенности. Тройка трассировки и распространение действий. Ведение журналов сообщений.

Методические указания к изучению

Рассматриваются вопросы использования трассировки на платформе WCF, ее особенности. Параметры настройки трассировки и способы ее проведения.

Литература: [1, с. 140–201], [3, с. 40–46].

Контрольные вопросы

1. Понятие трассировки и ее виды.
2. Базовая трассировка, настройка и использование.

3.8 Раздел 8. Инфраструктура безопасности

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

Перечень изучаемых вопросов: принципы обеспечения безопасности служб, основные сценарии безопасности и способы обеспечения защищенной передачи данных в распределенных приложениях, созданных на платформе WCF. Настройки безопасности на транспортном уровне и на уровне сообщений и особенности их использования. Выбор привязки для обеспечения безопасности, их характеристики и функциональные возможности.

Методические указания к изучению

Рассматриваются основные понятия безопасности служб, зависимость настроек безопасности от выбора привязки и способа размещения. Особенности безопасности сообщений и выбор привязки для такого способа обеспечения безопасности. Сравнительный анализ привязок при выборе политики безопасности.

Литература: [1, с. 240–301], [2, с. 136–187], [4, с. 38–44].

Контрольные вопросы

1. Какие способы обеспечения безопасности есть в WCF?
2. Чем отличается обеспечение безопасности транспорта от безопасности сообщений?
3. Какие параметры влияют на выбор привязки при создании распределенных защищенных приложений?

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

Перечень изучаемых вопросов: проверка подлинности и ее особенности при создании служб WCF, настройки политики безопасности и выбор сценария обеспечения безопасности для распределенных приложений. Способы аутентификации и проверки подлинности пользователей и службы, сертификаты безопасности.

Методические указания к изучению

Рассматриваются вопросы выбора способа проверки подлинности для службы и клиента при создании службы. Особенности политики безопасности для различных сценариев и размещения распределенного приложения.

Литература: [1, с. 140–201], [2, с. 236–287], [3, с. 40–46], [4, с. 36–54].

Контрольные вопросы

1. Какие бывают способы проверки подлинности клиента и службы?
2. Отличия различных типовых сценариев безопасности с точки зрения проверки подлинности клиента.
3. Каким образом производится проверка подлинности при помощи сертификатов безопасности?

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

Перечень изучаемых вопросов: авторизация и персонификация в службах WCF. Проверка подлинности и ее особенности при создании служб WCF, настройки политики безопасности и выбор сценария обеспечения безопасности для распределенных приложений. Способы аутентификации и проверки подлинности пользователей и службы, сертификаты безопасности.

Методические указания к изучению

Рассматриваются вопросы выбора способа проверки подлинности для службы и клиента при создании службы. Особенности политики безопасности для различных сценариев и размещения распределенного приложения. Особенности персонификации и настроек проверки подлинности с помощью маркеров безопасности.

Литература: [3, с. 40–46], [4, с. 36–54].

Контрольные вопросы

1. Какие бывают способы проверки подлинности клиента и службы?
2. Отличия различных типовых сценариев безопасности с точки зрения проверки подлинности клиента.
3. Каким образом производится проверка подлинности при помощи маркеров безопасности?

3.8.4 Тема 8.4 Свойства транзакций. Протоколы транзакций, Распространение транзакций. Транзакции и однонаправленные вызовы

Перечень изучаемых вопросов: транзакции, виды транзакций. Транзакции и безопасность в WCF. Основные протоколы транзакций и их выбор. Атрибуты для настройки транзакций. Способы создания транзакций и алгоритм программирования транзакций.

Методические указания к изучению

Рассматриваются вопросы использования транзакций при программировании распределенных приложений в WCF. Их основные свойства

и способы создания и настройки транзакций. Выбор протокола и настройки безопасности, предоставляемые платформой.

Литература: [1, с. 140–201], [2, с. 236–287], [3, с. 40–46], [4, с. 36–54].

Контрольные вопросы

1. Перечислить свойства транзакций.
2. Особенности протокола транзакций и их выбор.
3. Значения атрибутов транзакций и их настройка. Выбор прослушивателя транзакции.

4. МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО ПОДГОТОВКЕ К ЛАБОРАТОРНЫМ ЗАНЯТИЯМ

Лабораторные занятия направлены на углубление знаний и закрепление основных понятий и методов, изучаемых в рамках дисциплины. Основная цель занятий – научиться применять теоретические знания для решения прикладных задач.

Рекомендации к подготовке

1. Изучение лекционного материала и конспектов:

- перед лабораторными занятиями необходимо проработать соответствующие разделы лекционного материала;
- рекомендуется вести конспект занятий и дополнительно пересмотреть его перед началом лабораторного занятия.

2. Проработка учебной литературы:

- используйте основные учебники и методические пособия, рекомендованные преподавателем;
- для глубокого понимания теории рекомендуется обращаться к дополнительной литературе.

3. Решение типовых задач:

- проработать примеры и типовые задачи из учебных материалов, методических указаний;
- выполните задачи, предложенные преподавателем для самостоятельной работы, что обеспечит лучшее понимание методов и подходов к решению задач.

4. Подготовка вопросов:

- составьте список вопросов по материалу, вызвавшему затруднения;
- обсуждение этих вопросов на лабораторном занятии поможет устранить пробелы в знаниях.

5. Вопросы для самоконтроля:

- перед каждым занятием рекомендуется проверять себя с помощью вопросов для самоконтроля из методических указаний к лекционным занятиям. Это позволит оценить уровень своей подготовки.

Тематический план лабораторных занятий приводится в разделе «Тематический план».

Подробная информация по выполнению лабораторных работ и рекомендуемая литература приведены в УМП по выполнению лабораторных работ по дисциплине «Технология построения защищенных приложений для открытых систем».

5. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО САМОСТОЯТЕЛЬНОЙ РАБОТЕ

В лекциях по предмету излагаются основные знания по курсу дисциплины. Самостоятельная работа имеет особое значение для прочного усвоения материала. Она помогает научиться правильно, ориентироваться в научной литературе, самостоятельно мыслить и находить правильные ответы на возникающие вопросы. В ходе всех видов занятий происходит углубление и закрепление знаний студентов, вырабатывается умение правильно излагать свои мысли.

Самостоятельная работа выполняет ряд функций, к которым относятся:

- развивающая (повышение культуры умственного труда, приобщение к творческим видам деятельности, обогащение интеллектуальных способностей студентов);
- информационно-обучающая (учебная деятельность студентов на аудиторных занятиях, неподкрепленная самостоятельной работой, становится малорезультативной);
- ориентирующая и стимулирующая (процессу обучения придается профессиональное ускорение);
- воспитывающая (формируются и развиваются профессиональные качества специалиста);
- исследовательская (новый уровень профессионально-творческого мышления).

В основе самостоятельной работы студентов лежат принципы: самостоятельности, развивающе-творческой направленности, целевого планирования, личностно-деятельностного подхода.

Самостоятельная работа студентов проводится с целью:

- систематизации и закрепления полученных теоретических знаний и практических умений студентов;
- углубления и расширения теоретических знаний;
- формирования умений использовать нормативную, правовую, справочную документацию и специальную литературу;
- развития познавательных способностей и активности студентов: творческой инициативы, самостоятельности, ответственности и организованности;
- формирования самостоятельности мышления, способностей к саморазвитию, самосовершенствованию и самореализации;
- развития исследовательских умений.

Для достижения указанной цели студенты на основе плана самостоятельной работы должны решать следующие задачи:

- изучить рекомендуемые литературные источники;
- изучить основные понятия, представленные в глоссарии;
- ответить на контрольные вопросы;
- решить предложенные задачи, кейсы, ситуации;
- выполнить контрольные и курсовые работы.

Работа студентов в основном складывается из следующих элементов:

1. Изучение и усвоение в соответствии с учебным планом программного материала по всем учебным дисциплинам;
2. Выполнение письменных контрольных и курсовых работ;
3. Подготовка и сдача зачетов, курсовых работ, итоговых экзаменов;
4. Написание и защита дипломной работы.

Самостоятельная работа включает такие формы работы, как:

- индивидуальное занятие (домашние занятия) – важный элемент в работе студента по расширению и закреплению знаний;
- конспектирование лекций;
- получение консультаций для разъяснений по вопросам изучаемой дисциплины;
- подготовка ответов на вопросы тестов;
- подготовка к экзамену;
- выполнение контрольных, курсовых проектов и дипломных работ;
- подготовка научных докладов, рефератов, эссе;
- анализ деловых ситуаций (мини кейсов) и др.

Содержание внеаудиторной самостоятельной работы определяется в соответствии с рекомендуемыми видами заданий в соответствии с рабочей программой учебной дисциплины. Распределение объема времени на внеаудиторную самостоятельную работу в режиме дня студента не регламентируется расписанием.

Виды заданий для внеаудиторной самостоятельной работы, их содержание и характер могут иметь вариативный и дифференциальный характер, учитывать специфику специальности, изучаемой дисциплины, индивидуальные особенности студента.

Видами заданий для внеаудиторной самостоятельной работы могут быть:

– для овладения знаниями:

- чтение текста (учебника, первоисточника, дополнительной литературы);
- составление плана текста;
- конспектирование текста;
- выписки из текста;
- работа со словарями и справочниками;
- исследовательская работа;
- использование аудио- и видеозаписи;
- работа с электронными информационными ресурсами и ресурсами Internet;

– для закрепления и систематизации знаний:

- работа с конспектом лекции (обработка текста);
- повторная работа над учебным материалом (учебника, первоисточника, дополнительной литературы, аудиовидеозаписей);

- составление плана и тезисов ответа;
 - выполнение тестовых заданий;
 - ответы на контрольные вопросы;
 - аннотирование, реферирование, рецензирование текста;
 - подготовка сообщений к выступлению на семинаре, конференции;
- подготовка рефератов, докладов;
- работа с компьютерными программами;
 - подготовка к сдаче экзамена;
- для формирования умений:
- решение задач и упражнений по образцу;
 - решение вариативных задач и упражнений;
 - выполнение расчетно-графических работ;
 - решение ситуационных производственных (профессиональных) задач;
 - участие в научных и практических конференциях;
 - проектирование и моделирование разных видов и компонентов профессиональной деятельности;
 - создание проспектов, проектов, моделей;
 - экспериментальная работа, участие в НИР;
 - рефлексивный анализ профессиональных умений с использованием аудио- видеотехники и компьютерных расчетных программ и электронных практикумов;
 - подготовка курсовых проектов и дипломных работ.

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.

Вопросы и задачи для самопроверки:

1. Особенности создания распределенных приложений и использования распределенных вычислений.
2. Этапы развития технологии распределенных вычислений.
3. Основные платформы для создания распределенных приложений.
4. Обзор технологий, отличных от WCF ориентированных.
5. Как можно задать адрес, привязку и контракт для конечной точки?
6. Какие виды конечных точек бывают?
7. Особенности конфигурирования конечной точки клиента.
8. Какие способы обеспечения безопасности есть в WCF?
9. Чем отличается обеспечение безопасности транспорта от безопасности сообщений?
10. Какие параметры влияют на выбор привязки при создании распределенных защищенных приложений?

11. Что такое прокси-класс?
12. В чем отличие способов создания прокси-классов?
13. Как можно сгенерировать его вручную или динамически. Особенности, преимущества и недостатки?
14. Конечная точка службы, способа задания адреса, привязки, контракта.
15. Задание параметров конечной точки в файле конфигурации.
16. Понятие базовых адресов.

6. ТРЕБОВАНИЯ К АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ

6.1. Текущая аттестация

В ходе изучения дисциплины студентам предстоит пройти следующие этапы текущей аттестации: контроль самостоятельной работы по темам дисциплины, контроль выполнения лабораторных работ.

К оценочным средствам текущего контроля успеваемости относятся:

– тестовые задания открытого и закрытого типов.

Экзамен может проводиться как в традиционной форме, так и в виде экзаменационного тестирования. Тестовые задания для проведения экзаменационного тестирования приведены в фонде оценочных средств по дисциплине.

6.1.1 Критерии оценки результатов освоения дисциплины

Универсальная система оценивания результатов обучения включает в себя системы оценок: 1) «отлично», «хорошо», «удовлетворительно», «неудовлетворительно»; 2) «зачтено», «не зачтено»; 3) 100-балльную/процентную систему и правило перевода оценок в пятибалльную систему (таблица 2).

Таблица 2 – Система оценок и критерии выставления оценки

Система оценок Критерий	2	3	4	5
	0-40 %	41-60 %	61-80 %	81-100 %
	«неудовлетворительно»	«удовлетворительно»	«хорошо»	«отлично»
	«не зачтено»	«зачтено»		
1. Системность и полнота знаний в отношении изучаемых объектов	Обладает частичными и разрозненными знаниями, которые не может научно-корректно связывать	Обладает минимальным набором знаний, необходимым для системного взгляда на	Обладает набором знаний, достаточным для системного взгляда на изучаемый	Обладает полнотой знаний и системным взглядом на изучаемый объект

Система оценок Критерий	2	3	4	5
	0-40 %	41-60 %	61-80 %	81-100 %
	«неудовлетворительно»	«удовлетворительно»	«хорошо»	«отлично»
	«не зачтено»	«зачтено»		
	между собой (только некоторые из которых может связывать между собой)	изучаемый объект	объект	
2. Работа с информацией	Не в состоянии находить необходимую информацию, либо в состоянии находить отдельные фрагменты информации в рамках поставленной задачи	Может найти необходимую информацию в рамках поставленной задачи	Может найти, интерпретировать и систематизировать необходимую информацию в рамках поставленной задачи	Может найти, систематизировать необходимую информацию, а также выявить новые, дополнительные источники информации в рамках поставленной задачи
3. Научное осмысление изучаемого явления, процесса, объекта	Не может делать научно-корректных выводов из имеющихся у него сведений, в состоянии проанализировать только некоторые из имеющихся у него сведений	В состоянии осуществлять научно-корректный анализ предоставленной информации	В состоянии осуществлять систематический и научно-корректный анализ предоставленной информации, вовлекает в исследование новые релевантные данные	В состоянии осуществлять систематический и научно-корректный анализ предоставленной информации, вовлекает в исследование новые релевантные поставленной задаче данные, предлагает новые

Система оценок Критерий	2	3	4	5
	0-40 %	41-60 %	61-80 %	81-100 %
	«неудовлетворительно»	«удовлетворительно»	«хорошо»	«отлично»
	«не зачтено»	«зачтено»		
				ракурсы поставленной задачи
4. Освоение стандартных алгоритмов решения профессиональных задач	В состоянии решать только фрагменты поставленной задачи в соответствии с заданным алгоритмом, не освоил предложенный алгоритм, допускает ошибки	В состоянии решать поставленные задачи в соответствии с заданным алгоритмом	В состоянии решать поставленные задачи в соответствии с заданным алгоритмом, понимает основы предложенного алгоритма	Не только владеет алгоритмом и понимает его основы, но и предлагает новые решения в рамках поставленной задачи

6.1.2 Оценивание тестовых заданий закрытого типа осуществляется по системе зачтено/ не зачтено («зачтено» – 41–100 % правильных ответов; «не зачтено» – менее 40 % правильных ответов) или пятибалльной системе (оценка «неудовлетворительно» – менее 40 % правильных ответов; оценка «удовлетворительно» – от 41 до 60 % правильных ответов; оценка «хорошо» – от 61 до 80 % правильных ответов; оценка «отлично» – от 81 до 100 % правильных ответов).

Тестовые задания открытого типа оцениваются по системе «зачтено/не зачтено». Оценивается верность ответа по существу вопроса, при этом не учитывается порядок слов в словосочетании, верность окончаний, падежи.

6.1.3 Условия получения положительной оценки:

Завершающим этапом изучения дисциплины является итоговая аттестация, представляющая собой экзамен.

Тестовые задания для проведения тестирования приведены в фонде оценочных средств по дисциплине.

Допуск к итоговой аттестации возможен при:

- всех выполненных, сданных (проверенных, защищенных) лабораторных работах, наличии отчётов по ним;
- наличии показателей приемлемого уровня освоения материалов курса: более 50 % посещений от общего числа требуемых по учебному плану.

ПРИМЕРНЫЕ ВОПРОСЫ К ЭКЗАМЕНУ ПО ДИСЦИПЛИНЕ

1. Основные понятия WCF. Контракты. Привязки. Адреса.
2. Контракты служб. Контракты ошибок. Примеры.
3. Visual Studio. C#.
4. Шаблоны проектов WCF в Visual Studio.
5. Контракты данных. Коллекции.
6. Контракты сообщений. Пример.
7. Сериализация.
8. Суть конечных точек службы.
9. Создание конечных точек с помощью файла конфигурации. Базовые адреса.
10. Создание конечной точки с помощью программного кода. Публикация метаданных посредством конечных точек.
11. Общие сведения об архитектуре метаданных.
12. Настройка стандартных привязок. Нестандартные привязки.
13. Работа с базой данных Access.
14. Работа с Microsoft SQL Server 2005.
15. Использование утилиты svcutil для генерирования прокси-класса.
16. Использование среды Visual Studio для генерирования прокси-класса.
17. Определение прокси-класса вручную.
18. Динамическое создание прокси-класса.
19. Использование служб, отличных от WCF-ориентированных.
20. Конфигурирование конечной точки клиента.
21. Динамическое конфигурирование службы.
22. Базовая трассировка в WCF.
23. Сквозная трассировка.
24. Обеспечение безопасности на транспортном уровне.
25. Привязки и безопасность. Обеспечение безопасности на уровне сообщений.
26. Основы проверки подлинности. Политика безопасности.
27. Учетные данные клиентов. Учетные данные службы. Собственная проверка подлинности.
28. Учетные данные клиентов. Учетные данные в виде сертификата. Учетные данные в виде выдаваемых маркеров. Учетные данные Windows.
29. Авторизация и персонификация.
30. Авторизация. Авторизация на основе заявок. Проверка подлинности с помощью маркеров безопасности.
31. Персонификация.
32. Свойства транзакций. Протоколы транзакций.
33. Распространение транзакций. Транзакции и однонаправленные вызовы.
34. Программирование транзакций.

- 35. Обработка клиентских исключений.
- 36. Безопасность сообщений и безопасность транспорта. Сравнительные характеристики.
- 37. Обработка ошибок. Типы ошибок и способы их устранения
- 38. Основные сценарии безопасности в WCF и их особенности

7. ЗАКЛЮЧЕНИЕ

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.

В лекциях по предмету излагаются основные знания по курсу дисциплины. Самостоятельная работа имеет особое значение для прочного усвоения материала. Она помогает научиться правильно, ориентироваться в научной литературе, самостоятельно мыслить и находить правильные ответы на возникающие вопросы. В ходе всех видов занятий происходит углубление и закрепление знаний студентов, вырабатывается умение правильно излагать свои мысли.

Самостоятельная работа выполняет ряд функций, к которым относятся:

- развивающая (повышение культуры умственного труда, приобщение к творческим видам деятельности, обогащение интеллектуальных способностей студентов);
- информационно-обучающая (учебная деятельность студентов на аудиторных занятиях, не подкреплённая самостоятельной работой, становится малорезультативной);
- ориентирующая и стимулирующая (процессу обучения придается профессиональное ускорение);
- воспитывающая (формируются и развиваются профессиональные качества специалиста);
- исследовательская (новый уровень профессионально-творческого мышления).

В основе самостоятельной работы студентов лежат принципы: самостоятельности, развивающе-творческой направленности, целевого планирования, личностно-деятельностного подхода.

Самостоятельная работа студентов проводится с целью:

- систематизации и закрепления полученных теоретических знаний и практических умений студентов;
- углубления и расширения теоретических знаний;
- формирования умений использовать нормативную, правовую, справочную документацию и специальную литературу;
- развития познавательных способностей и активности студентов: творческой инициативы, самостоятельности, ответственности и организованности;
- формирования самостоятельности мышления, способностей к саморазвитию, самосовершенствованию и самореализации;
- развития исследовательских умений.

Для достижения указанной цели студенты на основе плана самостоятельной работы должны решать следующие задачи:

- изучить рекомендуемые литературные источники;
- изучить основные понятия, представленные в глоссарии;
- ответить на контрольные вопросы.

Работа студентов в основном складывается из следующих элементов:

- изучение и усвоение в соответствии с учебным планом программного материала по всем учебным дисциплинам;
- подготовка и сдача итогового зачета, экзамена.

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.

8. ЛИТЕРАТУРА

1. Информационная безопасность: учеб. пособие / В. И. Лойко, В. Н. Лаптев, Г. А. Аршинов, С. Н. Лаптев. – Краснодар: КубГАУ, 2020. – 332 с. – Режим доступа: для авториз. пользователей. – Лань : электронно-библиотечная система. – URL: <https://e.lanbook.com/book/254168> (дата обращения: 09.10.2024). – ISBN 978-5-907346-50-5. — Текст : электронный.
2. Нестеров, С. А. Основы информационной безопасности / С. А. Нестеров. – 3-е изд., стер. – Санкт-Петербург: Лань, 2024. – 324 с. – Режим доступа: для авториз. пользователей. – Лань : электронно-библиотечная система. – URL: <https://e.lanbook.com/book/370967> (дата обращения: 09.10.2024). – ISBN 978-5-507-49077-6. – Текст : электронный.
3. Программно-аппаратные средства защиты информации: учеб. пособие / С. А. Зырянов, М. А. Кувшинов, И. А. Огнев, И. В. Никрошкин. – Новосибирск: НГТУ, 2023. – 80 с. – Режим доступа: для авториз. пользователей. – Лань : электронно-библиотечная система. – URL: <https://e.lanbook.com/book/404549> (дата обращения: 10.12.2024). – ISBN 978-5-7782-4905-9. – Текст : электронный.
4. Пугин, В. В. Криптографические протоколы: учеб. пособие / В. В. Пугин. – Самара: ПГУТИ, 2019. – 68 с. – Режим доступа: для авториз. пользователей. – Лань : электронно-библиотечная система. – URL: <https://e.lanbook.com/book/223319> (дата обращения: 10.12.2024). – Текст : электронный.

Дополнительная литература

5. Красов, А. В. Разработка защищенного программного обеспечения: учеб. пособие / А. В. Красов, А. Ю. Цветков. – СанктПетербург: СПбГУТ им. М.А. Бонч-Бруевича, 2023. – 154 с. – Режим доступа: для авториз. пользователей. – Лань : электроннобиблиотечная система. – URL: <https://e.lanbook.com/book/425906> (дата обращения: 09.10.2024). – ISBN 978-5-89160-308-0. – Текст : электронный.
6. Раханов, К. Я. Обеспечение конфиденциальности информации в сети Интернет: учеб. пособие / К. Я. Раханов, Н. А. Раханова. – Новополюцк: ПГУ, 2021. – 192 с. – Режим доступа: для авториз. пользователей. – Лань : электронно-библиотечная система. – URL: <https://e.lanbook.com/book/366821> (дата обращения: 09.10.2024). – ISBN 978-985-531-723-5. – Текст : электронный.
7. Лозовецкий, В. В. Защита автоматизированных систем обработки информации и телекоммуникационных сетей: учеб. пособие для вузов / В. В. Лозовецкий, Е. Г. Комаров, В. В. Лебедев; под ред. В. В. Лозовецкий. – 2-е изд., стер. – Санкт-Петербург: Лань, 2024. – 488 с. – Режим доступа: для авториз. пользователей. – Лань : электронно-библиотечная система. – URL: <https://e.lanbook.com/book/397355> (дата обращения: 09.10.2024). – ISBN 978-5-507-47615-2. – Текст : электронный.

Периодические издания

8. «Безопасность информационных технологий», «Информационно-управляющие системы», «Информация и безопасность».

Учебно-методические пособия, нормативная литература

9. Бабаева А. А. Технология построения защищенных приложений для открытых систем: учеб-метод. пособие по изучению дисциплины для студентов специальности 10.05.03 «Информационная безопасность автоматизированных систем» / А. А. Бабаева. – Калининград: Изд-во ФГБОУ ВО «КГТУ», 2022. – 41 с. – URL: https://klgtu.ru/vikon/sveden/files/zih/UMP_Tehnologiya_postroeniya_zaschischennykh_priloghenii_dlya_otkrytykh_sistem.pdf (дата обращения: 09.10.2024). – Текст : электронный.

10. Бабаева, А. А. Технология построения защищенных приложений для открытых систем: учеб-метод. пособие по выполнению лаб. работ для студентов специальности 10.05.03 Информационная безопасность автоматизированных систем / А. А. Бабаева. – Калининград: Изд-во ФГБОУ ВО «КГТУ», 2022. – 120 с. — URL: [https://klgtu.ru/vikon/sveden/files/ait/UMP_Tehnologiya_postroeniya_zaschischennykh_priloghenii_dlya_otkrytykh_sistem_\(laboratornye_raboty\).pdf](https://klgtu.ru/vikon/sveden/files/ait/UMP_Tehnologiya_postroeniya_zaschischennykh_priloghenii_dlya_otkrytykh_sistem_(laboratornye_raboty).pdf) (дата обращения: 09.10.2024). — Текст : электронный.

11. Информационная безопасность распределенных информационных систем: метод. указания по выполнению лабораторных работ для студентов специальности 10.05.03 «Информационная безопасность автоматизированных систем» всех форм обучения / Федер. агентство по рыболовству [и др.]; сост. В. В. Подтопельный. – Калининград: БГАРФ, 2020. – Ч. 1. – 61 с. – Текст : непосредственный.

12. Информационная безопасность распределенных информационных систем: метод. указания по выполнению лаб. работ для студентов специальности 10.05.03 «Информ. безопасность автоматизир. систем» всех форм обучения / Федер. агентство по рыболовству [и др.]; сост. В. В. Подтопельный. – Калининград : БГАРФ, 2021. – Ч. 2. – 42 с. – Текст : непосредственный.

13. Информационная безопасность автоматизированных информационных систем : метод. указания по выполнению лаб. работ для студентов специальности 10.05.03 «Информ. безопасность автоматизир. систем» очной формы обучения / Федер. агентство по рыболовству [и др.]; авт.-сост. А. А. Бабаева. – изд. 2-е, с доп. изм. – Калининград: БГАРФ, 2022. – 46 с. – Текст : непосредственный.

14. Подтопельный, В. В. Системы защиты от утечки конфиденциальной информации: учеб.-метод. пособие по практическим работам дисциплины для студентов специальности 10.05.03 «Информационная безопасность автоматизированных систем». – Калининград: Изд-во ФГБОУ ВО «КГТУ», 2022. – 61 с. – URL: https://www.klgtu.ru/vikon/sveden/files/ziq/UMP_Sistemy_zaschity_o

t_utechki_konfidentialnoi_informacii_(laboratornye_raboty).pdf (дата обращения: 09.10.2024). – Текст : электронный.

Локальный электронный методический материал

Алина Андреевна Бабаева

ТЕХНОЛОГИЯ ПОСТРОЕНИЯ ЗАЩИЩЕННЫХ ПРИЛОЖЕНИЙ
ДЛЯ ОТКРЫТЫХ СИСТЕМ

Редактор С. Кондрашова
Корректор Т. Звада

Уч.-изд. л. 3,0. Печ. л. 2,4.

Издательство федерального государственного бюджетного
образовательного учреждения высшего образования
«Калининградский государственный технический университет».
236022, Калининград, Советский проспект, 1