ФГБОУ ВПО «Воронежский государственный
технический университет»

Кафедра систем информационной безопасности

215-2015

МЕТОДИЧЕСКИЕ УКАЗАНИЯ

к практическим занятиям по дисциплине
«Технология построения
защищенных распределенных приложений»
для студентов специальности
090303 «Информационная безопасность
автоматизированных систем»
очной формы обучения

Воронеж 2015

Составитель канд. техн. наук С. С. Куликов

УДК 004.05

Методические указания к практическим занятиям по дисциплине «Технология построения защищенных распределенных приложений» для студентов специальности 090303 «Информационная безопасность автоматизированных систем» очной формы обучения / ФГБОУ ВПО «Воронежский государственный технический университет»; сост. С. С. Куликов. Воронеж, 2015. 15 с.

Методические указания к практическим занятиям содержат задания по разработке специализированного программного обеспечения, демонстрирующего основные методы и средства обеспечения взаимодействия компонентов проектируемых распределенных приложений и обеспечения их безопасности.

Методические указания подготовлены в электронном виде в текстовом редакторе MW-2013 и содержатся в файле Куликов_ПЗ_ТПЗРП.pdf.

Библиогр.: 5 назв.

Рецензент д-р техн. наук, проф. А. Г. Остапенко

Ответственный за выпуск зав. кафедрой д-р техн. наук, проф. А. Г. Остапенко

Издается по решению редакционно-издательского совета Воронежского государственного технического университета

ВВЕДЕНИЕ

Методические указания предназначены для студентов очной формы обучения, изучающих дисциплину «Технология построения защищенных распределенных приложений» и содержат методический материал, содержащий практические задания, контрольные вопросы и рекомендуемую литературу.

В процессе выполнения практической работы необходимо создать приложение, демонстрирующее знание студентом технологий, методов и средств обеспечения взаимодействия компонент распределенных приложений или обеспечения безопасности распределенных приложений, а также ответить на контрольные вопросы, приведенные в каждой практической работе.

Выполнение заданий проверяется преподавателем в ходе практического занятия, а проверка ответов на контрольные вопросы – при защите практической работы.

Практическое занятие № 1
Сокеты

Цель занятия

Разработка распределенного приложения с взаимодействием компонент через программный интерфейс сокетов.

Задание

На базе класса Socket пространства имен System.Net.Sockets программной платформы .NET Framework разработать два приложения, удаленно взаимодействующих между собой через программный интерфейс сокетов.

Контрольные вопросы

1. Раскройте понятие и перечислите типы сокетов.
2. Раскройте понятие и объясните назначение сетевого адреса и сетевого порта.
3. Объясните предназначение и опишите структуру класса Socket.
4. Объясните предназначение и опишите структуру класса IPHostEntry.
5. Объясните предназначение и опишите структуру класса IPAddress.
6. Объясните предназначение и опишите структуру класса IPEndPoint.
7. Объясните предназначение и опишите структуру класса MulticastOption.
8. Объясните предназначение и опишите структуру класса SocketException.

Практическое занятие № 2
Одноранговые сети

Цель занятия

Разработка распределенного приложения с взаимодействием компонент через программный интерфейс сокетов.

Задание

На базе класса Cloud пространства имен System.Net.PeerToPeer программной платформы .NET Framework разработать два приложения, удаленно взаимодействующих между собой в рамках одноранговой сети через «облако».

Контрольные вопросы

1. Сформулируйте основы функционирования и технологии построения одноранговых сетей.
2. Объясните предназначение и опишите структуру протоколов FEC и MDC.
3. Перечислите проблемы безопасности одноранговых сетей.
4. Объясните предназначение и опишите структуру класса Cloud.
5. Объясните предназначение и опишите структуру класса CloudCollection.
6. Объясните предназначение и опишите структуру класса PeerName.
7. Объясните предназначение и опишите структуру класса PeerNameRegistration.
8. Объясните предназначение и опишите структуру класса PeerToPeerException.

Практическое занятие № 3
Промежуточная среда обмена сообщениями MSMQ

Цель занятия

Разработка распределенного приложения с взаимодействием компонент через промежуточную среду MSMQ.

Задание

На базе класса MessageQueue пространства имен System.Messaging программной платформы .NET Framework разработать два приложения, удаленно взаимодействующих между собой через промежуточную среду обмена сообщениями MSMQ.

Контрольные вопросы

1. Поясните принципы работы службы обмена сообщениями MSMQ.
2. Перечислите инфраструктуру, необходимую для использования MSMQ.
3. Объясните применение службы сообщений MSMQ в распределенных приложениях.
4. Объясните предназначение и опишите структуру класса MessageQueue.
5. Объясните предназначение и опишите структуру класса MessageEnumerator.
6. Объясните предназначение и опишите структуру класса Message.
7. Объясните предназначение и опишите структуру класса MessagePropertyFilter.
8. Объясните предназначение и опишите структуру класса MessageQueueException.

Практическое занятие № 4
Промежуточная среда COM+

Цель занятия

Разработка распределенного приложения с взаимодействием компонент через промежуточную среду COM+.

Задание

На базе класса ServicedComponent пространства имен System.EnterpriseServices программной платформы .NET Framework разработать два приложения, удаленно взаимодействующих между собой через промежуточную среду COM+.

Контрольные вопросы

1. Опишите архитектуру среды COM+.
2. Перечислите сервисы COM+.
3. Объясните предназначение и опишите структуру класса ServicedComponent.
4. Объясните предназначение и опишите структуру класса AutoCompleteAttribute.
5. Объясните предназначение и опишите структуру класса ContextUtil.
6. Объясните предназначение и опишите структуру класса RegistrationHelper.
7. Объясните предназначение и опишите структуру класса ServicedComponentException.

Практическое занятие № 5
Промежуточная среда веб-служб ASP .NET

Цель занятия

Разработка распределенного приложения с взаимодействием компонент через промежуточную среду ASP.NET.

Задание

На базе класса WebService пространства имен System.Web.Services программной платформы .NET Framework разработать два приложения, удаленно взаимодействующих между собой через промежуточную среду веб-служб ASP.NET.

Контрольные вопросы

1. Опишите архитектуру веб-службы ASP.NET.
2. Объясните использование расширения WSE.
3. Объясните предназначение и опишите структуру класса WebService.
4. Объясните предназначение и опишите структуру класса WebMethodAttribute.
5. Объясните предназначение и опишите структуру класса WebServiceAttribute.
6. Объясните предназначение и опишите структуру класса WebServiceBindingAttribute.
7. Объясните предназначение и опишите структуруперечисления WsiProfiles.

Практическое занятие № 6
Промежуточная среда .NET Remoting

Цель занятия

Разработка распределенного приложения с взаимодействием компонент через промежуточную среду .NET Remoting.

Задание

На базе классов и нтерфейсов пространств имен System.Runtime.Remoting и System.Runtime.Remoting.Messaging программной платформы .NET Framework разработать два приложения, удаленно взаимодействующих между собой через промежуточную среду .NET Remoting.

Контрольные вопросы

1. Опишите сценарии использования среды Remoting.
2. Опишите архитектуру среды .NET Remoting.
3. Объясните конфигурирование среды .NET Remoting.
4. Опишите канал среды Remoting.
5. Объясните процесс создания нестандартного канала.
6. Объясните предназначение и опишите структуру класса TransparentProxy.
7. Объясните предназначение и опишите структуру класса RealProxy.

Практическое занятие № 7
Генерация случайных чисел

Цель занятия

Разработка приложения, реализующего алгоритм генерации псевдослучайных чисел.

Задание

1. На базе класса Random пространства имен System программной платформы .NET Framework разработать приложение, генерирующее псевдослучайное число.
2. На базе класса RNGCryptoServiceProvider пространства имен System.Security.Cryptography программной платформы .NET Framework разработать приложение, генерирующее псевдослучайное число.

Контрольные вопросы

1. Раскройте понятие псевдослучайного числа.
2. Перечислите возможные источники энтропии.
3. Перечислите основные законы распределения случайных чисел.
4. Объясните предназначение и опишите структуру статистических тестов NIST.
5. Объясните предназначение и опишите структуру класса Random.
6. Объясните предназначение и опишите структуру класса RandomNumberGenerator.
7. Объясните предназначение и опишите структуру класса RNGCryptoServiceProvider.

Практическое занятие № 8
Хеширование

Цель занятия

Разработка приложения, реализующего алгоритмы хеширования.

Задание

1. На базе одного из классов: MD5, RIPEMD160Managed, SHA1, SHA256, SHA384 или SHA512 пространства имен System.Security.Cryptography программной платформы .NET Framework разработать приложение, хеширующее данные.
2. На базе одного из классов: HMACMD5, HMACRIPEMD160, HMACSHA1, HMACSHA256, HMACSHA384 или HMACSHA512 пространства имен System.Security.Cryptography программной платформы .NET Framework разработать приложение, вычисляющее хэш-код проверки подлинности данных с использования алгоритма хеширования.

Контрольные вопросы

1. Раскройте понятие и назначение хеширования.
2. Раскройте понятие и назначение HMAC.
3. Объясните предназначение и опишите структуру класса HashAlgorithm.
4. Объясните предназначение и опишите структуру класса KeyedHashAlgorithm.
5. Объясните предназначение и опишите структуру класса MD5.
6. Объясните предназначение и опишите структуру класса HMACMD5.

7. Объясните предназначение и опишите структуру класса SHA1.

8. Объясните предназначение и опишите структуру класса HMACSHA1.

Практическое занятие № 9
Симметричное шифрование

Цель занятия

Разработка приложения, реализующего алгоритм симметричного шифрования.

Задание

На базе одного из классов: AesManaged, AesCryptoServiceProvider, DESCryptoServiceProvider, RC2CryptoServiceProvider, RijndaelManaged или TripleDESCryptoServiceProvider пространства имен System.Security.Cryptography программной платформы .NET Framework разработать приложение, шифрующее данные.

Контрольные вопросы

1. Объясните предназначение и опишите структуру класса SymmetricAlgorithm.
2. Объясните предназначение и опишите структуру класса AesCryptoServiceProvider.
3. Объясните предназначение и опишите структуру класса AesManaged.
4. Объясните предназначение и опишите структуру класса DESCryptoServiceProvider.
5. Объясните предназначение и опишите структуру класса RC2CryptoServiceProvider.
6. Объясните предназначение и опишите структуру класса RijndaelManaged.
7. Объясните предназначение и опишите структуру класса TripleDESCryptoServiceProvider.

Практическое занятие № 10
Асимметричное шифрование

Цель занятия

Разработка приложения, реализующего алгоритм асимметричного шифрования.

Задание

На базе класса RSACryptoServiceProvider пространства имен System.Security.Cryptography программной платформы .NET Framework разработать приложение, шифрующее данные, предварительно создав пару асимметричных ключей.

Контрольные вопросы

1. Объясните предназначение и опишите структуру класса AsymmetricAlgorithm.
2. Объясните предназначение и опишите структуру класса RSA.
3. Объясните предназначение и опишите структуру класса RSACryptoServiceProvider.
4. Объясните предназначение и опишите структуру класса CspParameters.
5. Объясните предназначение и опишите структуру класса CryptoKeySecurity.
6. Объясните предназначение и опишите структуру класса RSAParameters.
7. Объясните предназначение и опишите структуру класса CryptographicException.

Практическое занятие № 11
Цифровые подписи

Цель занятия

Разработка приложений, реализующих алгоритмы формирования и проверки цифровых подписей.

Задание

1. На базе класса DSACryptoServiceProvider или ECDsaCng пространства имен System.Security.Cryptography программной платформы .NET Framework разработать приложение, формирующее цифровую подпись для данных.
2. На базе класса DSACryptoServiceProvider или ECDsaCng пространства имен System.Security.Cryptography программной платформы .NET Framework разработать приложение, проверяющее цифровую подпись для данных.

Контрольные вопросы

1. Объясните предназначение и опишите содержания PKCS #7.
2. Объясните предназначение и опишите содержания Стандарт RFC 5652.
3. Объясните предназначение и опишите содержания Положения приказа ФСБ от 27.12.2011 г. N 795.
4. Объясните предназначение и опишите структуру класса AsymmetricAlgorithm.
5. Объясните предназначение и опишите структуру класса DSACryptoServiceProvider.
6. Объясните предназначение и опишите структуру класса CspParameters.
7. Объясните предназначение и опишите структуруперечисления ECKeyXmlFormat.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Рихтер, Д. CLR via C#. Программирование на платформе Microsoft .NET Framework 2.0 на языке C# [Текст] / Д. Рихтер. – М.: Питер, 2007. – 636 с.

2. Троелсен, Э. Язык программирования C# 2010 и платформа .NET 4.0 [Текст] / Э. Троелсен. – М.: Вильямс, 2010. – 1392 с.

3. Павловская, Т. C#. Программирование на языке высокого уровня [Текст] / Т. Павловская. – М.: Питер, 2007. – 432 с.

4. Основы криптографии [Текст]: учеб. пособие / А. П. Алферов, А. К. Зубов, А. С. Кузьмин, А. В. Черемушкин. – М.: Гелиос АРВ, 2002. – 480 с.

5. Шнайер, Б. Прикладная криптография [Текст] / Б. Шнайер. – М.: Триумф, 2003. – 816 с.

СОДЕРЖАНИЕ

МЕТОДИЧЕСКИЕ УКАЗАНИЯ

к практическим занятиям по дисциплине
«Технология построения
защищенных распределенных приложений»
для студентов специальности
090303 «Информационная безопасность
автоматизированных систем»
очной формы обучения

Составитель
Куликов Сергей Сергеевич

В авторской редакции

Подписано к изданию 27.04.2015.

Уч.-изд. л. 0,9.

ФГБОУВПО «Воронежский государственный
технический университет»
394026 Воронеж, Московский просп., 14