МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное учреждение
высшего профессионального образования
"Казанский (Приволжский) федеральный университет"
Институт вычислительной математики и информационных технологий

УТВЕРЖДАЮ

Проректор по образовательной деятельности КФУ

Проф. Таюрский Д.А.

_____ _____ 20___ г.

подписано электронно-цифровой подписью

Программа дисциплины

Криптография Б3.ДВ.7

Направление подготовки: 010400.62 - Прикладная математика и информатика
Профиль подготовки: Математическое и информационное обеспечение экономической деятельности
Квалификация выпускника: бакалавр
Форма обучения: очное
Язык обучения: русский

Автор(ы):

Пинягина О.В.

Рецензент(ы):

Андрианова А.А.

СОГЛАСОВАНО:

Заведующий(ая) кафедрой: Миссаров М. Д.
Протокол заседания кафедры No ___ от "____" _____ 201__г
Учебно-методическая комиссия Института вычислительной математики и информационных технологий:
Протокол заседания УМК No ____ от "____" _____ 201__г

Регистрационный No 966916

Казань
2016

Содержание

Программу дисциплины разработал(а)(и) доцент, к.н. (доцент) Пинягина О.В. кафедра анализа данных и исследования операций отделение фундаментальной информатики и информационных технологий , Olga.Piniaguina@kpfu.ru

1. Цели освоения дисциплины

В рамках данного спецкурса изучаются практические вопросы реализации криптографических и иных, связанных с безопасностью, функциональных возможностей в приложениях .NET.

2. Место дисциплины в структуре основной образовательной программы высшего профессионального образования

Данная учебная дисциплина включена в раздел " Б3.ДВ.7 Профессиональный" основной образовательной программы 010400.62 Прикладная математика и информатика и относится к дисциплинам по выбору. Осваивается на 4 курсе, 8 семестр.

Дисциплина изучается на 4 курсе, в 8 семестре.

Для изучения данного курса студент должен изучить курс "Основы программирования в C#"

3. Компетенции обучающегося, формируемые в результате освоения дисциплины /модуля

В результате освоения дисциплины формируются следующие компетенции:

Шифр компетенции	Расшифровка приобретаемой компетенции
ПК-4 (профессиональные компетенции)	способность в составе научно-исследовательского и производственного коллектива решать задачи профессиональной деятельности;
ПК-8 (профессиональные компетенции)	способность формировать суждения о значении и последствиях своей профессиональной деятельности с учетом социальных, профессиональных и этических позиций;
ПК-9 (профессиональные компетенции)	способность решать задачи производственной и технологической деятельности на профессиональном уровне, включая: разработку алгоритмических и программных решений в области системного и прикладного программирования;

В результате освоения дисциплины студент:

1. должен знать:

2. должен уметь:

3. должен владеть:

- понять и освоить базовые концепции платформы .NET Security,

- приобрести практические навыки, необходимые для обращения с функциональными возможностями .NET, предназначенными для разработки программ с использованием криптографии и других технологий обеспечения безопасности.
- применять на практике криптографические возможности среды .NET,
- разрабатывать клиент-серверные приложения с применением технологий шифрования.

- понять и освоить базовые концепции платформы .NET Security,
- приобрести практические навыки, необходимые для обращения с функциональными возможностями .NET, предназначенными для разработки программ с использованием криптографии и других технологий обеспечения безопасности.
- применять на практике криптографические возможности среды .NET,
- разрабатывать клиент-серверные приложения с применением технологий шифрования.

4. Структура и содержание дисциплины/ модуля

Общая трудоемкость дисциплины составляет 2 зачетных(ые) единиц(ы) 72 часа(ов).

Форма промежуточного контроля дисциплины зачет в 8 семестре.

Суммарно по дисциплине можно получить 100 баллов, из них текущая работа оценивается в 50 баллов, итоговая форма контроля - в 50 баллов. Минимальное количество для допуска к зачету 28 баллов.

86 баллов и более - "отлично" (отл.);

71-85 баллов - "хорошо" (хор.);

55-70 баллов - "удовлетворительно" (удов.);

54 балла и менее - "неудовлетворительно" (неуд.).

4.1 Структура и содержание аудиторной работы по дисциплине/ модулю

Тематический план дисциплины/модуля

N	Раздел Дисциплины/ Модуля	Семестр	Неделя семестра	Виды и часы аудиторной работы, их трудоемкость (в часах)			Текущие формы контроля
				Лекции	Практические занятия	Лабораторные работы	
1.	Тема 1. Криптография и безопасность в .NET.	8	1-2	0	5	0	домашнее задание
2.	Тема 2. Основы криптографии.	8	3-4	0	5	0	домашнее задание

N	Раздел Дисциплины/ Модуля	Семестр	Неделя семестра	Виды и часы аудиторной работы, их трудоемкость (в часах)			Текущие формы контроля
				Лекции	Практические занятия	Лабораторные работы	
3.	Тема 3. Симметричная криптография.	8	5-6	0	5	0	творческое задание домашнее задание
4.	Тема 4. Асимметричная криптография.	8	7-9	0	5	0	творческое задание домашнее задание
5.	Тема 5. Цифровая подпись. Хеш-алгоритмы.	8	10-12	0	5	0	творческое задание домашнее задание
6.	Тема 6. Криптография и XML.	8	13-14	0	5	0	домашнее задание творческое задание
7.	Тема 7. Концепция безопасности, основанной на идентификации пользователей в .NET.	8	15-16	0	5	0	творческое задание домашнее задание
8.	Тема 8. ASP.NET. Базовые механизмы безопасности.	8	17-18	0	5	0	домашнее задание творческое задание
.	Тема . Итоговая форма контроля	8		0	0	0	зачет
	Итого			0	40	0	

4.2 Содержание дисциплины

Тема 1. Криптография и безопасность в .NET.

практическое занятие (5 часа(ов)):

Криптография и безопасность в .NET. Природа криптографии и других средств обеспечения безопасности. Безопасность в Windows: возраст зрелости. Среда разработки .NET Framework и "виртуальная машина" CRL. Программирование с использованием криптографии в .NET. Программирование с использованием средств обеспечения безопасности в .NET.

Тема 2. Основы криптографии.

практическое занятие (5 часа(ов)):

Основы криптографии. Основные термины криптографии. Секретные ключи против секретных алгоритмов. Классические методы сохранения тайны. Стеганография. Современные шифры. Симметричная криптография. Асимметричная криптография. Криптографические алгоритмы. Криптографические протоколы. Криптоаналитические атаки.

Тема 3. Симметричная криптография.

практическое занятие (5 часа(ов)):

Симметричная криптография. Симметричные шифры. DES. Тройной DES. Rijndael. Основные криптографические классы - класс SymmetricAlgorithm и производные от него. Проблемы передачи ключей. Шифрованные хеши и целостность сообщения. Хеш-алгоритмы с ключом и целостность сообщения

Тема 4. Асимметричная криптография.

практическое занятие (5 часа(ов)):

Асимметричная криптография. Проблемы, связанные с использованием симметричных алгоритмов: проблема распределения ключей и проблема доверия. Идея асимметричной криптографии. RSA: самый распространенный асимметричный алгоритм. Программирование при помощи .NET Asymmetric Cryptography. Сохранение ключей в формате XML. Цифровые сертификаты

Тема 5. Цифровая подпись. Хеш-алгоритмы.

практическое занятие (5 часа(ов)):

Цифровая подпись. Хеш-алгоритмы. Характеристики хорошей хеш-функции. Класс HashAlgorithm. Классы MD5 и SHA. Класс KeyedHashAlgorithm. RSA в качестве алгоритма цифровой подписи. Алгоритм цифровой подписи DSA Иерархия класса AsymmetricAlgorithm. Класс DSACryptoServiceProvider

Тема 6. Криптография и XML.

практическое занятие (5 часа(ов)):

Криптография и XML. XML Encryption - шифрование XML. XML Signatures - подпись XML.

Тема 7. Концепция безопасности, основанной на идентификации пользователей в .NET.

практическое занятие (5 часа(ов)):

Концепция безопасности, основанной на идентификации пользователей в .NET. Аутентификация и авторизация. Модель безопасности .NET. Администрирование безопасности на уровне Windows. Администрирование безопасности на уровне .NET. Безопасность, основанная на идентификации пользователей. Императивный подход. Декларативный подход. Мандаты. Дисциплина безопасности.

Тема 8. ASP.NET. Базовые механизмы безопасности.

практическое занятие (5 часа(ов)):

ASP.NET. Базовые механизмы безопасности. Аутентификация. Авторизация. Реализация механизма аутентификации в ASP.NET. Конфигурация ASP.NET. Аутентификация при помощи формы. Классы для аутентификации при помощи форм. Аутентификация при помощи паспорта.

4.3 Структура и содержание самостоятельной работы дисциплины (модуля)

N	Раздел Дисциплины	Семестр	Неделя семестра	Виды самостоятельной работы студентов	Трудоемкость (в часах)	Формы контроля самостоятельной работы
1.	Тема 1. Криптография и безопасность в .NET.	8	1-2	подготовка домашнего задания	4	домашнее задание
2.	Тема 2. Основы криптографии.	8	3-4	подготовка домашнего задания	4	домашнее задание
3.	Тема 3. Симметричная криптография.	8	5-6	подготовка домашнего задания	3	домашнее задание
				подготовка презентации и доклада	1	творческое задание

N	Раздел Дисциплины	Семестр	Неделя семестра	Виды самостоятельной работы студентов	Трудоемкость (в часах)	Формы контроля самостоятельной работы
4.	Тема 4. Асимметричная криптография.	8	7-9	подготовка домашнего задания	3	домашнее задание
				подготовка презентации и доклада	1	творческое задание
5.	Тема 5. Цифровая подпись. Хеш-алгоритмы.	8	10-12	подготовка домашнего задания	3	домашнее задание
				подготовка презентации и доклада	1	творческое задание
6.	Тема 6. Криптография и XML.	8	13-14	подготовка домашнего задания	3	домашнее задание
				подготовка презентации и доклада	1	творческое задание
7.	Тема 7. Концепция безопасности, основанной на идентификации пользователей в .NET.	8	15-16	подготовка домашнего задания	3	домашнее задание
				подготовка презентации и доклада	1	творческое задание
8.	Тема 8. ASP.NET. Базовые механизмы безопасности.	8	17-18	подготовка домашнего задания	3	домашнее задание
				подготовка презентации и доклада	1	творческое задание
	Итого				32	

5. Образовательные технологии, включая интерактивные формы обучения

Практические занятия, подготовка презентации, выступление с докладом, зачет.

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

Тема 1. Криптография и безопасность в .NET.

домашнее задание , примерные вопросы:

Изучение курса должно завершаться выполнением индивидуального проекта - клиент-серверного приложения с применением технологий шифрования. В качестве языка программирования требуется использовать C#, среда разработки может быть любой. Проект состоит из серверного и клиентского модулей. Желательно, чтобы клиентский модуль представлял собой оконное приложение, а для серверного модуля это не обязательно. На этом этапе требуется выбрать предметную область и сформулировать концептуальную схему будущего приложения.

Тема 2. Основы криптографии.

домашнее задание , примерные вопросы:

Задание на тему "Ввод-вывод в .Net". Пусть текстовый файл содержит пары 'логин-пароль'. Напишите программу, которая по заданному логину находит и печатает пароль или сообщение о том, что логин не найден.

Тема 3. Симметричная криптография.

домашнее задание , примерные вопросы:

Задание на тему "Сериализация": Напишите программу, которая сериализует и десериализует произвольный объект в файл. Используйте обычный формат XML и формат SOAP. Просмотрите полученные XML-файлы в любом текстовом редакторе или браузере.

творческое задание , примерные вопросы:

Изучение литературы по курсу, а также подготовка презентации и доклад на семинарских занятиях на одну из выбранных тем (не менее 1 презентации и доклада на студента в семестр).

Тема 4. Асимметричная криптография.

домашнее задание , примерные вопросы:

Задание на тему "Сетевое программирование": Создайте простые приложения клиент и сервер на основе классов TcpListener и TcpClient. Пусть, например, клиент отправляет сообщение, сервер его принимает и в ответ тоже отправляет сообщение, и на этом сеанс клиента завершается.

творческое задание , примерные вопросы:

Изучение литературы по курсу, а также подготовка презентации и доклад на семинарских занятиях на одну из выбранных тем (не менее 1 презентации и доклада на студента в семестр).

Тема 5. Цифровая подпись. Хеш-алгоритмы.

домашнее задание , примерные вопросы:

Создайте оконное приложение для клиента.

творческое задание , примерные вопросы:

Изучение литературы по курсу, а также подготовка презентации и доклад на семинарских занятиях на одну из выбранных тем (не менее 1 презентации и доклада на студента в семестр).

Тема 6. Криптография и XML.

домашнее задание , примерные вопросы:

Подключите многопотоковость к вашим серверному и клиентскому приложениям.

творческое задание , примерные вопросы:

Изучение литературы по курсу, а также подготовка презентации и доклад на семинарских занятиях на одну из выбранных тем (не менее 1 презентации и доклада на студента в семестр).

Тема 7. Концепция безопасности, основанной на идентификации пользователей в .NET.

домашнее задание , примерные вопросы:

Включите в ваше приложение работу с базой данных. К базе данных, разумеется, может обращаться только сервер, но не клиент.

творческое задание , примерные вопросы:

Изучение литературы по курсу, а также подготовка презентации и доклад на семинарских занятиях на одну из выбранных тем (не менее 1 презентации и доклада на студента в семестр).

Тема 8. ASP.NET. Базовые механизмы безопасности.

домашнее задание , примерные вопросы:

Включите в ваше клиент-серверное приложение возможности шифрования. Примеры клиент-серверных приложений с шифрованием: 1. чат (система обмена текстовыми сообщениями) с шифрованием всех сообщений; 2. приложение для клиентов банка, позволяющее обмениваться зашифрованными сообщениями с оператором банка, а также пересылать конфиденциальные документы; 3. корпоративная система обмена сообщениями, в которой не требуется секретности, но обязательно обеспечить целостность сообщений с помощью технологии цифровой подписи.

творческое задание , примерные вопросы:

Изучение литературы по курсу, а также подготовка презентации и доклад на семинарских занятиях на одну из выбранных тем (не менее 1 презентации и доклада на студента в семестр).

Тема . Итоговая форма контроля

Примерные вопросы к зачету:

В течение семестра каждый студент должен подготовить доклад на одну из предложенных тем (в виде презентации) и выступить с ним на семинаре. Кроме того, предполагается выполнение каждым студентом текущих заданий и индивидуального проекта. Базовая тема индивидуального проекта - сетевое приложение (консольное или оконное) с архитектурой клиент-сервер, применяющее какие-либо из криптографических возможностей .NET.

Применение проектного подхода и творческих заданий не предусматривает проведение контрольных работ.

Вопросы к зачету по курсу "Криптография и безопасность в .NET. "

1. Природа криптографии и других средств обеспечения безопасности.
2. Безопасность в Windows: возраст зрелости.
3. Среда разработки .NET Framework и "виртуальная машина" CRL.
4. Программирование с использованием криптографии в .NET.
5. Программирование с использованием средств обеспечения безопасности в .NET.
6. Основы криптографии. Основные термины криптографии.
7. Секретные ключи против секретных алгоритмов.
8. Классические методы сохранения тайны.
9. Стеганография. Современные шифры.
10. Криптоаналитические атаки.
11. Симметричная криптография. Симметричные шифры. DES. Тройной DES. Rijndael.
12. Основные криптографические классы - класс SymmetricAlgorithm и производные от него.
13. Шифрованные хеши и целостность сообщения. Хеш-алгоритмы с ключом и целостность сообщения
14. Асимметричная криптография.
15. Проблемы, связанные с использованием симметричных алгоритмов: проблема распределения ключей и проблема доверия.
16. Идея асимметричной криптографии. RSA: самый распространенный асимметричный алгоритм.
17. Программирование при помощи .NET Asymmetric Cryptography.
18. Сохранение ключей в формате XML.
19. Цифровые сертификаты
20. Цифровая подпись. Хеш-алгоритмы. Характеристики хорошей хеш-функции.
21. Класс HashAlgorithm. Классы MD5 и SHA. Класс KeyedHashAlgorithm.
22. RSA в качестве алгоритма цифровой подписи.
23. Алгоритм цифровой подписи DSA.
24. Иерархия класса AsymmetricAlgorithm. Класс DSACryptoServiceProvider
25. XML Encryption - шифрование XML.
26. XML Signatures - подпись XML.
27. Концепция безопасности, основанной на идентификации пользователей в .NET.
28. Аутентификация и авторизация.
29. Модель безопасности .NET.
30. Администрирование безопасности на уровне Windows.
31. Администрирование безопасности на уровне .NET.
32. Безопасность, основанная на идентификации пользователей.

33. Императивный подход.
34. Декларативный подход.
35. Мандаты. Дисциплина безопасности.
36. ASP.NET. Базовые механизмы безопасности. Аутентификация. Авторизация.
37. Реализация механизма аутентификации в ASP.NET.
38. Конфигурация ASP.NET.
39. Аутентификация при помощи формы.
40. Классы для аутентификации при помощи форм.
41. Аутентификация при помощи паспорта.

7.1. Основная литература:

1.Криптографические методы защиты информации. Том 3: Учебно-методическое пособие / А.В. Бабаш. - 2-е изд. - М.: ИЦ РИОР: НИЦ ИНФРА-М, 2014. - 216 с.: 60x88 1/8. - (Высшее образование: Бакалавриат). (обложка) ISBN 978-5-369-01304-5, 200

http://www.znanium.com/bookread.php?book=432654

2.Глухов М.М. Пичкур А.Б. Черемушкин А.В. Введение в теоретико-числовые методы криптографии. - Санкт-Петербург: Лань, 2011. - 400 с.

http://e.lanbook.com/books/element.php?pl1_id=1540

3. Червяков Н.И., Евдокимов А.А., Галушкин А.И., Лавриненко И.Н. Применение искусственных нейронных сетей и системы остаточных классов в криптографии. - М.: Физматлит, 2012. - 280с.

http://e.lanbook.com/books/element.php?pl1_id=5300

4.Введение в теоретико-числовые методы криптографии : учебное пособие для студентов высших учебных заведений, обучающихся по специальности 090101 "Криптография" / М. М. Глухов, И. А. Круглов, А. Б. Пичкур, А. В. Черемушкин .? Санкт-Петерург [и др.] : Лань, 2011 .? 394 с. ; 21 см. ? (Учебники для вузов, Специальная литература) .? Библиогр.: с. 382-389 .? ISBN 978-5-8114-1116-0 ((в пер.)) , 1000.

7.2. Дополнительная литература:

1. Ишмухаметов Ш.Т. Математические основы защиты информации: учебное пособие, 2012. - URL: http://kpfu.ru/docs/F366166681/mzi.pdf

Башлы, П. Н. Информационная безопасность и защита информации [Электронный ресурс]: Учебник / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. - М.: РИОР, 2013. - 222 с. http://znanium.com/bookread.php?book=405000

7.3. Интернет-ресурсы:

MSDN - информационный сервис для разработчиков - http://msdn.microsoft.com

Криптография и безопасность в .NET - электронный ресурс - http://kek.ksu.ru/EOS/crypt/index.html

Методические указания для студентов - http://kek.ksu.ru/EOS/crypt/MetodUkaz.doc

Основы C# - http://kek.ksu.ru/EOS/CDiez/index.html

Регламент курса - http://kek.ksu.ru/EOS/crypt/reglament.doc

8. Материально-техническое обеспечение дисциплины(модуля)

Освоение дисциплины "Криптография" предполагает использование следующего материально-технического обеспечения:

лабораторные занятия проводятся в компьютерном классе, оснащенном интерактивной доской.

Программа составлена в соответствии с требованиями ФГОС ВПО и учебным планом по направлению 010400.62 "Прикладная математика и информатика" и профилю подготовки Математическое и информационное обеспечение экономической деятельности .

Автор(ы):
Пинягина О.В. _____
"__" _____ 201 __ г.

Рецензент(ы):
Андрианова А.А. _____
"__" _____ 201 __ г.