

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



подписано электронно-цифровой подписью

Программа дисциплины

Теория кодирования информации и криптография Б3.ДВ.5

Направление подготовки: 010300.62 - Фундаментальная информатика и информационные технологии

Профиль подготовки: Системный анализ и информационные технологии

Квалификация выпускника: бакалавр

Форма обучения: очное

Язык обучения: русский

Автор(ы):

Латыпов Р.Х. , Разинков Е.В.

Рецензент(ы):

Ишмухаметов Ш.Т.

СОГЛАСОВАНО:

Заведующий(ая) кафедрой: Латыпов Р. Х.

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 916514

Казань
2014

Содержание

1. Цели освоения дисциплины
2. Место дисциплины в структуре основной образовательной программы
3. Компетенции обучающегося, формируемые в результате освоения дисциплины /модуля
4. Структура и содержание дисциплины/ модуля
5. Образовательные технологии, включая интерактивные формы обучения
6. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины и учебно-методическое обеспечение самостоятельной работы студентов
7. Литература
8. Интернет-ресурсы
9. Материально-техническое обеспечение дисциплины/модуля согласно утвержденному учебному плану

Программу дисциплины разработал(а)(и) директор института вычислительной математики Латыпов Р.Х. Директорат Института ВМ и ИТ Институт вычислительной математики и информационных технологий , Roustam.Latypov@kpfu.ru ; ассистент, к.н. Разинков Е.В. кафедра системного анализа и информационных технологий отделение фундаментальной информатики и информационных технологий , Evgenij.Razinkov@kpfu.ru

1. Цели освоения дисциплины

Спецкурс, читаемый студентам четвертого курса, должен преследовать следующие цели.

1. Ввести слушателей читателя в те области арифметики, как классические, так и самые современные, которые находятся в центре внимания приложений теории чисел, особенно криптографии. Предполагается, что знание высшей алгебры и теории чисел ограничено самым скромным знакомством с их основами; по этой причине излагаются также необходимые сведения из этих областей математики. Авторами избран алгоритмический подход, причем особое внимание уделяется оценкам эффективности методов, предлагаемых теорией.
2. Ознакомить студентов с основными достижениями теории помехоустойчивого кодирования: существующие ограничения и основные линейные коды: Хэмминга, БЧХ, Рида-Маллера, Рида-Соломона.
3. Значительное внимание уделяется изучению широко используемых криптографических алгоритмов симметричного и асимметричного шифрования, а также криптографических хэш-функций.

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

Данная учебная дисциплина включена в раздел " Б3.ДВ.5 Профессиональный" основной образовательной программы 010300.62 Фундаментальная информатика и информационные технологии и относится к дисциплинам по выбору. Осваивается на 4 курсе, 7 семестр.

Данная дисциплина относится к профессиональным дисциплинам.

Читается на 4 курсе в 7 семестре для студентов обучающихся по направлению "Фундаментальная информатика и информационные технологии".

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

В результате освоения дисциплины формируются следующие компетенции:

Шифр компетенции	Расшифровка приобретаемой компетенции
ПК-2 (профессиональные компетенции)	способность профессионально решать задачи производственной и технологической деятельности с учетом современных достижений науки и техники, включая: разработку алгоритмических и программных решений в области системного и прикладного программирования; разработку математических, информационных и имитационных моделей по тематике выполняемых исследований; создание информационных ресурсов глобальных сетей, образовательного контента, прикладных баз данных; разработку тестов и средств тестирования систем и средств на соответствие стандартам и исходным требованиям; разработку эргономических человеко-машинных интерфейсов (в соответствии с профилизацией)

Шифр компетенции	Расшифровка приобретаемой компетенции
ПК-5 (профессиональные компетенции)	способность в составе научно-исследовательского и производственного коллектива решать задачи профессиональной деятельности (в соответствии с профилем подготовки)
ПК-7 (профессиональные компетенции)	способность применять на практике международные и профессиональные стандарты информационных технологий, современные парадигмы и методологии, инструментальные и вычислительные средства (в соответствии с профилем подготовки)
ПК-8 (профессиональные компетенции)	способность профессионально владеть базовыми математическими знаниями и информационными технологиями, эффективно применять их для решения научно-технических задач и прикладных задач, связанных с развитием и использованием информационных технологий

В результате освоения дисциплины студент:

1. должен знать:

- основные результаты теории чисел и алгебры, понимать проблемы сложности алгоритмов
- основные аспекты безопасности и основные угрозы безопасности

2. должен уметь:

- ориентироваться в вопросах стандартов безопасности и законодательства в области защиты информации

3. должен владеть:

- знаниями по основным разделам теории кодирования и криптографии

4. должен демонстрировать способность и готовность:

- применять полученные знания в своей профессиональной деятельности.

4. Структура и содержание дисциплины/ модуля

Общая трудоемкость дисциплины составляет 4 зачетных(ые) единиц(ы) 144 часа(ов).

Форма промежуточного контроля дисциплины экзамен в 7 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. Сложность алгоритмов	7		2	1	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	
2.	Тема 2. Сведения из теории чисел	7		2	1	0	домашнее задание
3.	Тема 3. Алгебраические структуры, конечные поля	7		3	1	0	домашнее задание
4.	Тема 4. Линейные блочные коды, границы помехоустойчивого кодирования. Код Хэмминга.	7		3	2	0	домашнее задание
5.	Тема 5. Циклические коды. Аппаратная реализация кодирования и декодирования. Коды БЧХ.	7		3	2	0	домашнее задание
6.	Тема 6. Мажоритарное декодирование и коды Рида-Маллера. Недвоичные коды и коды Рида-Соломона.	7		3	1	0	домашнее задание
7.	Тема 7. Аспекты безопасности, основные угрозы. Стандарты и законодательство в области безопасности.	7		3	1	0	домашнее задание
8.	Тема 8. Симметричное шифрование: докомпьютерные шифры.	7		3	1	0	домашнее задание
9.	Тема 9. Обзор результатов Клода Шеннона	7		2	1	0	домашнее задание
10.	Тема 10. Симметричное шифрование: обзор современных шифров.	7		2	1	0	домашнее задание
11.	Тема 11. Ассимметричное шифрование: односторонние функции и новые задачи криптографии.	7		2	1	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	
12.	Тема 12. Проблема распределения ключей и протоколы распределения ключей.	7		2	1	0	домашнее задание
13.	Тема 13. Система шифрования RSA	7		2	1	0	домашнее задание
14.	Тема 14. Протоколы проверки аутентичности, протоколы распределения секрета, протоколы цифровой подписи.	7		2	2	0	домашнее задание
15.	Тема 15. Протокол электронного голосования	7		2	1	0	домашнее задание
	Тема . Итоговая форма контроля	7		0	0	0	экзамен
	Итого			36	18	0	

4.2 Содержание дисциплины

Тема 1. Сложность алгоритмов

лекционное занятие (2 часа(ов)):

Экспоненциальная сложность. Полиномиальная сложность. O-нотация.

практическое занятие (1 часа(ов)):

Оценка сложности известных алгоритмов.

Тема 2. Сведения из теории чисел

лекционное занятие (2 часа(ов)):

Наибольший общий делитель. Алгоритм Евклида. Расширенный алгоритм Евклида. Китайская теорема об остатках. Функция Эйлера.

практическое занятие (1 часа(ов)):

Программная реализация решения системы уравнений по китайской теореме об остатках.

Тема 3. Алгебраические структуры, конечные поля

лекционное занятие (3 часа(ов)):

Кольца. Группы. Конечные поля, поля Галуа.

практическое занятие (1 часа(ов)):

Программная реализация вычислений в полях Галуа.

Тема 4. Линейные блочные коды, границы помехоустойчивого кодирования. Код Хэмминга.

лекционное занятие (3 часа(ов)):

Двоичный код. Расстояние Хэмминга. Кодовое расстояние. Линейный код. Порождающая матрица. Проверочная матрица. Код Хэмминга и его свойства.

практическое занятие (2 часа(ов)):

Построение кода Хэмминга.

Тема 5. Циклические коды. Аппаратная реализация кодирования и декодирования. Коды BCH.

лекционное занятие (3 часа(ов)):

Определение циклического кода, свойства. Архитектура кодера и декодера для циклического кода. Код Боуза-Чоудхури-Хоквингема.

практическое занятие (2 часа(ов)):

Программная реализация построения порождающего полинома циклического кода.

Тема 6. Мажоритарное декодирование и коды Рида-Маллера. Недвоичные коды и коды Рида-Соломона.

лекционное занятие (3 часа(ов)):

Мажоритарное декодирование линейных кодов. Коды Рида-Маллера, их свойства. Недвоичные циклические коды. Код Рида-Соломона, его свойства.

практическое занятие (1 часа(ов)):

Программная реализация кода Рида-Соломона.

Тема 7. Аспекты безопасности, основные угрозы. Стандарты и законодательство в области безопасности.

лекционное занятие (3 часа(ов)):

Конфиденциальность, целостность, доступность информации. Классификация атак. Классификация угроз. ГОСТ в области информационной безопасности.

практическое занятие (1 часа(ов)):

Анализ современных атак на программное обеспечение.

Тема 8. Симметричное шифрование: докомпьютерные шифры.

лекционное занятие (3 часа(ов)):

Шифр сдвига. Шифр замены. Шифр Виженера. Перестановочные шифры. Одноразовый шифр-блокнот.

практическое занятие (1 часа(ов)):

Программная реализация шифра замены.

Тема 9. Обзор результатов Клода Шеннона

лекционное занятие (2 часа(ов)):

Теоретико-информационная стойкость. Энтропия.

практическое занятие (1 часа(ов)):

Вычисление энтропии дискретного распределения.

Тема 10. Симметричное шифрование: обзор современных шифров.

лекционное занятие (2 часа(ов)):

Алгоритм AES. Алгоритм 3DES. Алгоритм RC4.

практическое занятие (1 часа(ов)):

Реализация алгоритма 3DES.

Тема 11. Ассимметричное шифрование: односторонние функции и новые задачи криптографии.

лекционное занятие (2 часа(ов)):

Задача факторизации. Задача вычисления дискретного логарифма.

практическое занятие (1 часа(ов)):

Реализация алгоритма быстрого возведения в степень по модулю.

Тема 12. Проблема распределения ключей и протоколы распределения ключей.

лекционное занятие (2 часа(ов)):

Протокол широкооротой лягушки. Протокол Нидхейма-Шредера. Протокол Отвэй-Риса.

практическое занятие (1 часа(ов)):

Программная реализация протокола Нидхейма-Шредера.

Тема 13. Система шифрования RSA

лекционное занятие (2 часа(ов)):

Задача факторизации. Вычисление модуля RSA. Выбор открытой экспоненты. Вычисление секретной экспоненты. Шифрование RSA. Расшифрование RSA. Стойкость алгоритма RSA.

практическое занятие (1 часа(ов)):

Программа реализации эффективного алгоритма расшифрования RSA.

Тема 14. Протоколы проверки аутентичности, протоколы распределения секрета, протоколы цифровой подписи.

лекционное занятие (2 часа(ов)):

Разделение секрета. Алгоритм DSA. Подпись Шнорра. Подпись Ниберга-Руппеля.

практическое занятие (2 часа(ов)):

Реализация алгоритма DSA.

Тема 15. Протокол электронного голосования

лекционное занятие (2 часа(ов)):

Установки системы. Заполнение бюллетеня. Распределение бюллетеней. Проверка достоверности информации. Подсчет голосов.

практическое занятие (1 часа(ов)):

Анализ стойкости системы электронного голосования.

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. Сложность алгоритмов	7		подготовка домашнего задания	3	домашнее задание
2.	Тема 2. Сведения из теории чисел	7		подготовка домашнего задания	3	домашнее задание
3.	Тема 3. Алгебраические структуры, конечные поля	7		подготовка домашнего задания	4	домашнее задание
4.	Тема 4. Линейные блочные коды, границы помехоустойчивого кодирования. Код Хэмминга.	7		подготовка домашнего задания	5	домашнее задание
5.	Тема 5. Циклические коды. Аппаратная реализация кодирования и декодирования. Коды БЧХ.	7		подготовка домашнего задания	5	домашнее задание

N	Раздел Дисциплины	Семестр	Неделя семестра	Виды самостоятельной работы студентов	Трудоемкость (в часах)	Формы контроля самостоятельной работы
6.	Тема 6. Мажоритарное декодирование и коды Рида-Маллера. Недвоичные коды и коды Рида-Соломона.	7		подготовка домашнего задания	4	домашнее задание
7.	Тема 7. Аспекты безопасности, основные угрозы. Стандарты и законодательство в области безопасности.	7		подготовка домашнего задания	4	домашнее задание
8.	Тема 8. Симметричное шифрование: докомпьютерные шифры.	7		подготовка домашнего задания	4	домашнее задание
9.	Тема 9. Обзор результатов Клода Шеннона	7		подготовка домашнего задания	3	домашнее задание
10.	Тема 10. Симметричное шифрование: обзор современных шифров.	7		подготовка домашнего задания	3	домашнее задание
11.	Тема 11. Ассимметричное шифрование: односторонние функции и новые задачи криптографии.	7		подготовка домашнего задания	3	домашнее задание
12.	Тема 12. Проблема распределения ключей и протоколы распределения ключей.	7		подготовка домашнего задания	3	домашнее задание
13.	Тема 13. Система шифрования RSA	7		подготовка домашнего задания	3	домашнее задание
14.	Тема 14. Протоколы проверки аутентичности, протоколы распределения секрета, протоколы цифровой подписи.	7		подготовка домашнего задания	4	домашнее задание
15.	Тема 15. Протокол электронного голосования	7		подготовка домашнего задания	3	домашнее задание
	Итого				54	

5. Образовательные технологии, включая интерактивные формы обучения

Обучение происходит в форме лекционных и практических занятий, а также самостоятельной работы студентов.

Теоретический материал излагается на лекциях. Причем конспект лекций, который остается у студента в результате прослушивания лекции не может заменить учебник. Его цель - формулировка основных утверждений и определений. Прослушав лекцию, полезно ознакомиться с более подробным изложением материала в учебнике. Список литературы разделен на две категории: необходимый для сдачи экзамена минимум и дополнительная литература.

Изучение курса подразумевает овладение теоретическим материалом и получение практических навыков для более глубокого понимания разделов дисциплины "Теория кодирования информации и криптография" на основе решения задач и упражнений, иллюстрирующих доказываемые теоретические положения, а также развитие абстрактного мышления и способности самостоятельно доказывать частные утверждения.

Самостоятельная работа предполагает выполнение домашних работ. Практические задания, выполненные в аудитории, предназначены для указания общих методов решения задач определенного типа. Закрепить навыки можно лишь в результате самостоятельной работы. Кроме того, самостоятельная работа включает подготовку к экзамену. При подготовке к сдаче экзамена весь объем работы рекомендуется распределять равномерно по дням, отведенным для подготовки к экзамену, контролировать каждый день выполнения работы. Лучше, если можно перевыполнить план. Тогда всегда будет резерв времени.

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

Тема 1. Сложность алгоритмов

домашнее задание , примерные вопросы:

Оценить сложность следующих алгоритмов: умножение Карацубы, алгоритм быстрого возведения в степень, алгоритм Евклида.

Тема 2. Сведения из теории чисел

домашнее задание , примерные вопросы:

Найти наибольший общий делитель двух чисел. Найти обратный элемент по модулю. Вычислить функцию Эйлера.

Тема 3. Алгебраические структуры, конечные поля

домашнее задание , примерные вопросы:

Доказать, что множество полиномов степени, не превосходящей n , является кольцом. Показать, что множество целых чисел является кольцом, но не является мультипликативной группой.

Тема 4. Линейные блочные коды, границы помехоустойчивого кодирования. Код Хэмминга.

домашнее задание , примерные вопросы:

Программная реализация кода Хэмминга.

Тема 5. Циклические коды. Аппаратная реализация кодирования и декодирования. Коды БЧХ.

домашнее задание , примерные вопросы:

Программная реализация кодов БЧХ.

Тема 6. Мажоритарное декодирование и коды Рида-Маллера. Недвоичные коды и коды Рида-Соломона.

домашнее задание , примерные вопросы:

Программная реализация кодов Рида-Маллера.

Тема 7. Аспекты безопасности, основные угрозы. Стандарты и законодательство в области безопасности.

домашнее задание , примерные вопросы:

Изучение государственных стандартов в области информационной безопасности.

Тема 8. Симметричное шифрование: докомпьютерные шифры.

домашнее задание , примерные вопросы:

Программная реализация шифра Виженера.

Тема 9. Обзор результатов Клода Шеннона

домашнее задание , примерные вопросы:

Написание программы, позволяющей оценить энтропию введенного текста.

Тема 10. Симметричное шифрование: обзор современных шифров.

домашнее задание , примерные вопросы:

Программная реализация алгоритма AES.

Тема 11. Ассимметричное шифрование: односторонние функции и новые задачи криптографии.

домашнее задание , примерные вопросы:

Реализовать алгоритм умножения Карацубы для двух больших чисел.

Тема 12. Проблема распределения ключей и протоколы распределения ключей.

домашнее задание , примерные вопросы:

Программная реализация протокола широкоротой лягушки.

Тема 13. Система шифрования RSA

домашнее задание , примерные вопросы:

Программная реализация алгоритма RSA.

Тема 14. Протоколы проверки аутентичности, протоколы распределения секрета, протоколы цифровой подписи.

домашнее задание , примерные вопросы:

Программная реализация протокола разделения секрета.

Тема 15. Протокол электронного голосования

домашнее задание , примерные вопросы:

Программная реализация протокола электронного голосования.

Тема . Итоговая форма контроля

Примерные вопросы к экзамену:

Контрольная работа 1:

Реализовать расширенный алгоритм Евклида.

Контрольная работа 2:

Программная реализация шифра RC4.

Экзаменационная программа:

1. Конфиденциальность, целостность, доступность информации. Классификация атак. Классификация угроз.
2. Экспоненциальная сложность. Полиномиальная сложность.
3. O-нотация
4. Кольцо, определение.
5. Группа, определение.
6. Поля Галуа.
7. Кольцо вычетов.
8. Доказать, что множество Z_n является кольцом.

9. Мультипликативная группа.
10. Доказать, что множество Z_n^* является мультипликативной группой.
11. Наибольший общий делитель.
12. Алгоритм Евклида.
13. Расширенный алгоритм Евклида.
14. Функция Эйлера.
15. Теорема Эйлера.
16. Китайская теорема об остатках.
17. Двоичный код.
18. Расстояние Хэмминга.
19. Кодовое расстояние.
20. Линейный код.
21. Порождающая и проверочная матрицы линейного кода.
22. Код Хэмминга и его свойства.
23. Определение циклического кода, свойства.
24. Архитектура кодера и декодера для циклического кода.
25. Код Боуза-Чоудхури-Хоквингема.
26. Мажоритарное декодирование линейных кодов.
27. Коды Рида-Маллера, их свойства.
28. Недвоичные циклические коды.
29. Код Рида-Соломона, его свойства.
30. Шифр сдвига.
31. Шифр замены.
32. Шифр Виженера.
33. Перестановочные шифры.
34. Одноразовый шифр-блокнот.
35. Теоретико-информационная стойкость. Энтропия.
36. Алгоритм шифрования AES.
37. Алгоритм шифрования 3DES.
38. Алгоритм шифрования RC4.
39. Задача факторизации.
40. Задача дискретного логарифмирования.
41. Протокол широкооротой лягушки.
42. Протокол Нидхейма-Шредера.
43. Протокол Отвэй-Риса.
44. Алгоритм шифрования RSA.
45. Эффективная реализация расшифрования RSA.
46. Атака на RSA: разделенный модуль.
47. Атака на RSA: малая шифрующая экспонента.
48. Атака на RSA: метод факторизации Ферма.
49. Схемы разделение секрета.
50. Алгоритм DSA.
51. Подпись Шнорра.
52. Подпись Ниберга-Руппеля.
53. Протокол электронного голосования.

Типовой экзаменационный билет:

1. Порождающая и проверочная матрицы линейного кода.

2. Алгоритм шифрования RSA.

7.1. Основная литература:

1. Громкович, Ю. Теоретическая информатика: Введение в теорию автоматов, теорию вычислимости, теорию сложности, теорию алгоритмов, рандомизацию, теорию связи и криптографию / Юрай Громкович; Пер. с нем.; Под ред. Б. Ф. Мельникова. ?Издание 3-е. ?Санкт-Петербург: БХВ-Петербург, 2010. ?336 с.
2. Латыпов Р.Х. Электронный образовательный ресурс "Кодирование информации и криптография - Математические основы", 2012 - <http://zilant.kpfu.ru/course/view.php?id=3>
3. Червяков Н.И., Евдокимов А.А., Галушкин А.И. Применение искусственных нейронных сетей и системы остаточных классов в криптографии. - - М.: Физматлит, 2012. - 280 с. URL: http://e.lanbook.com/books/element.php?pl1_id=5300
4. Кнауб, Л. В. Теоретико-численные методы в криптографии [Электронный ресурс] : Учеб. пособие / Л. В. Кнауб, Е. А. Новиков, Ю. А. Шитов. - Красноярск : Сибирский федеральный университет, 2011. - 160 с. URL: <http://znanium.com/bookread.php?book=441493>
5. Информационная безопасность: Учебное пособие / Т.Л. Партыка, И.И. Попов. - 5-е изд., перераб. и доп. - М.: Форум: НИЦ ИНФРА-М, 2014. - 432 с. URL: <http://znanium.com/bookread.php?book=420047>

7.2. Дополнительная литература:

Криптография, Сمارт, Н., 2006г.

Теория информации, Ляшева, Стелла Альбертовна;Ризаев, Ильдус Султанович;Шлеймович, Михаил Петрович, 2013г.

7.3. Интернет-ресурсы:

Википедия - <http://ru.wikipedia.org>

Интернет-портал математических образовательных ресурсов - <http://www.math.ru/>

Интернет-портал образовательных ресурсов КФУ - <http://www.kfu-elearning.ru/>
<http://www.kfu-elearning.ru/>

Интернет-портал со статьями по математике, алгоритмике и программированию - <http://algolist.manual.ru/>

Компьютерная энциклопедия - <http://www.computer-encyclopedia.ru>

8. Материально-техническое обеспечение дисциплины(модуля)

Освоение дисциплины "Теория кодирования информации и криптография" предполагает использование следующего материально-технического обеспечения:

Учебно-методическая литература для данной дисциплины имеется в наличии в электронно-библиотечной системе "ZNANIUM.COM", доступ к которой предоставлен студентам. ЭБС "ZNANIUM.COM" содержит произведения крупнейших российских учёных, руководителей государственных органов, преподавателей ведущих вузов страны, высококвалифицированных специалистов в различных сферах бизнеса. Фонд библиотеки сформирован с учетом всех изменений образовательных стандартов и включает учебники, учебные пособия, УМК, монографии, авторефераты, диссертации, энциклопедии, словари и справочники, законодательно-нормативные документы, специальные периодические издания и издания, выпускаемые издательствами вузов. В настоящее время ЭБС ZNANIUM.COM соответствует всем требованиям федеральных государственных образовательных стандартов высшего профессионального образования (ФГОС ВПО) нового поколения.

Лекции по дисциплине проводятся в аудитории, оснащенной доской и мелом(маркером), практические занятия проводятся в компьютерном классе.

Программа составлена в соответствии с требованиями ФГОС ВПО и учебным планом по направлению 010300.62 "Фундаментальная информатика и информационные технологии" и профилю подготовки Системный анализ и информационные технологии .

Автор(ы):

Латыпов Р.Х. _____

Разинков Е.В. _____

"__" _____ 201__ г.

Рецензент(ы):

Ишмухаметов Ш.Т. _____

"__" _____ 201__ г.