МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«Уральский федеральный университет имени первого Президента России Б.Н.Ельцина»

УТВЕРЖДАЮ
Проректор по учебной работе

_____ С.Т. Князев

«___» _____ 2018 г.

РАБОЧАЯ ПРОГРАММА МОДУЛЯ

Методы защиты информационных технических систем

Перечень сведений о рабочей программе модуля	**Учетные данные**
Модуль *Методы защиты информационных технических систем*	**Код модуля** 1140368
Образовательная программа *Информационные системы в научно-технических и социально-экономических технологиях*	**Код ОП 09.03.02/01.01** **Учебный план № 5456**
Траектория образовательной программы (ТОП)	*ТОП3* *Безопасность технических информационных систем*
Направление подготовки *Информационные системы и технологии*	**Код направления и уровня подготовки** *09.03.02*
Уровень подготовки *Бакалавр*	
ФГОС ВО	**Реквизиты приказа Минобрнауки РФ об утверждении ФГОС ВО**: *Приказ от 12.03.2015, №219*

Екатеринбург, 2018

Программа модуля составлена авторами:

№ п/п	ФИО	Ученая степень, ученое звание	Должность	Кафедра	Подпись
1	Звонарев К.В.	к.ф.-м.н.	доцент	Технической физики	

Руководитель модуля К.В. Звонарев

Рекомендовано учебно-методическим советом физико-технологического института

Председатель учебно-методического совета В.В. Зверев
Протокол № _____ от _____ г.

Согласовано:

Дирекция образовательных программ Р.Х. Токарева

Руководитель образовательной программы (ОП), для которой реализуется модуль

С.Л. Гольдштейн

1. ОБЩАЯ ХАРАКТЕРИСТИКА МОДУЛЯ

Методы защиты информационных технических систем

1.1. Объем модуля: 15 з.е.

1.2. Аннотация содержания модуля

Модуль «Методы защиты информационных технических систем» относится к вариативной части образовательной программы (по выбору студента) и направлен на формирование результатов обучения, связанных со способностью осуществлять в рамках научно-исследовательской и инновационной деятельности сбор, анализ научно-технической информации, отечественного и зарубежного опыта по тематике исследования; осуществлять в рамках производственно-технологической деятельности разработку и внедрение информационных технологий в технической физике, ядерной энергетике; осуществлять в рамках сервисно-эксплуатационной деятельности обеспечение безопасности и целостности данных информационных систем технологических предприятий. Модуль также направлен на формирование компетенций, непосредственно связанных с навыками защиты информации в информационно-технических системах. Модуль состоит из четырех дисциплин: «Безопасность баз данных», «Безопасность компьютерных сетей», «Криптографические методы защиты информации», «Основы теории алгоритмов и анализа их сложности».

Изучение дисциплины «Безопасность баз данных» позволит студентам ознакомиться с методами работы с современными реляционными СУБД, с методами обеспечения их безопасности, целостности и доступности, а также с принципами проектирования баз данных. Изучаются различные методы обеспечения высокой доступности и отказоустойчивости – технология резервного копирования и восстановления данных, репликация данных, различные способы обеспечения аппаратной избыточности. В процессе освоения дисциплины «*Безопасность компьютерных сетей*» студентам предоставляется возможность получить комплексное всестороннее представление о принципах построения систем защиты информации в вычислительных сетях. Рассматриваются подсистемы аутентификации и разграничения доступа в вычислительных сетях, безопасность сетевых протоколов, различные виды сетевых атак и защиты от них. В рамках дисциплины «*Криптографические методы защиты информации*» происходит изучение основ теории криптографической защиты информации. Студенты обучаются практическому применению криптографической защиты информации на базе современных крипто алгоритмов, овладевают методами реализации прикладных задач криптографии на базе языков программирования и пакетов прикладных программ. Изучение дисциплины «*Основы теории алгоритмов и анализа их сложности*» позволит студентам ознакомиться с основами математической логики, теорией алгоритмов, методами оценки сложности алгоритмов и построения эффективных алгоритмов. Полученные в рамках дисциплины «*Основы теории алгоритмов и анализа их сложности*» знания могут использоваться при проектировании новых и анализе существующих подсистем защиты в информационно-технических системах.

В результате успешного освоения модуля студенты получают теоретически и практические навыки обеспечения безопасности в информационно-технических системах.

2. СТРУКТУРА МОДУЛЯ И РАСПРЕДЕЛЕНИЕ УЧЕБНОГО ВРЕМЕНИ ПО ДИСЦИПЛИНАМ

Наименования дисциплин с указанием, к какой части образовательной программы они относятся: базовой (Б), вариативной – по выбору вуза (ВВ), вариативной - по выбору студента (ВС).		Семестр изучения	Объем времени, отведенный на освоение дисциплин модуля							
			Аудиторные занятия, час.				Самостоятельная работа, включая все виды текущей аттестации, час.	Промежуточная аттестация (зачет, экзамен), час.	Всего по дисциплине	
			Лекции	Практические занятия	Лабораторные работы	Всего			Часов	Зач. ед.
1.	**(ВС)** *Безопасность баз данных*	7	34		17	51	53	Зачет, 4	108	3
2.	**(ВС)** *Безопасность компьютерных сетей*	8	16		32	48	56	Зачет, 4	108	3
3.	**(ВС)** *Криптографические методы защиты информации*	8	32		32	64	134	Экзамен, 18	216	6
4.	**(ВС)** *Основы теории алгоритмов и анализа их сложности*	7	34		17	51	39	Экзамен, 18	108	3
Всего на освоение модуля			116	0	98	214	282	44	540	15

3. ПОСЛЕДОВАТЕЛЬНОСТЬ ОСВОЕНИЯ ДИСЦИПЛИН В МОДУЛЕ

3.1.	**Пререквизиты и постреквизиты в модуле**	-
3.2.	**Кореквизиты**	*Безопасность баз данных, Безопасность компьютерных сетей, Криптографические методы защиты информации, Основы теории алгоритмов и анализа их сложности*

4. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОСВОЕНИЯ МОДУЛЯ

4.1. Планируемые результаты освоения модуля и составляющие их компетенции

Коды ОП, для которых реализуется модуль	Планируемые в ОХОП результаты обучения -РО, которые формируются при освоении модуля	Компетенции в соответствии с ФГОС ВО
09.03.02/01.01	РО-О4 Способность осуществлять в рамках научно-исследовательской и инновационной	способностью использовать основные законы естественнонаучных дисциплин в профессиональной деятельности, применять методы математического анализа и моделирования, теоретического и экспериментального исследования (ОПК-2);

	деятельности сбор, анализ научно-технической информации, отечественного и зарубежного опыта по тематике исследования	способностью использовать математические методы обработки, анализа и синтеза результатов профессиональных исследований (ПК-25);
09.03.02/01.01	РО-О5 Способность использовать методологию экспериментальных исследований с целью проверки математических моделей, выбора оптимального решения задачи проектирования в рамках проектно-технологической и производственно-технологической деятельности	способностью разрабатывать средства автоматизированного проектирования информационных технологий (ПК-13); способностью использовать технологии разработки объектов профессиональной деятельности в областях: машиностроение, приборостроение, техника, образование, медицина, административное управление, юриспруденция, бизнес, предпринимательство, коммерция, менеджмент, банковские системы, безопасность информационных систем, управление технологическими процессам, механика, техническая физика, энергетика, ядерная энергетика, силовая электроника, металлургия, строительство, транспорт, железнодорожный транспорт, связь, телекоммуникации, управление инфокоммуникациями, почтовая связь, химическая промышленность, сельское хозяйство, текстильная и легкая промышленность, пищевая промышленность, медицинские и биотехнологии, горное дело, обеспечение безопасности подземных предприятий и производств, геология, нефтегазовая отрасль, геодезия и картография, геоинформационные системы, лесной комплекс, химико-лесной комплекс, экология, сфера сервиса, системы массовой информации, дизайн, медиаиндустрия, а также предприятия различного профиля и все виды деятельности в условиях экономики информационного общества (ПК-17);
09.03.02/01.01	РО-О6 Способность применять современные методы разработки компонентов информационных и технических систем в рамках производственно-технологической деятельности	способностью участвовать в работах по доводке и освоению информационных технологий в ходе внедрения и эксплуатации информационных систем (ПК-15);
09.03.02/01.01	РО-ТОП3-1 Способность осуществлять в рамках	способностью участвовать в работах по доводке и освоению информационных технологий в ходе внедрения и эксплуатации информационных

	производственно-технологической деятельности разработку и внедрение информационных технологий в технической физике, ядерной энергетике	систем (ПК-15); способностью использовать технологии разработки объектов профессиональной деятельности в областях: безопасность информационных систем, управление технологическими процессами, техническая физика, энергетика, ядерная энергетика, в условиях экономики информационного общества (ПК-17);
09.03.02/01.01	РО-ТОП3-2 Способность осуществлять в рамках сервисно-эксплуатационной деятельности обеспечение безопасности и целостности данных информационных систем технологических предприятий	способностью поддерживать работоспособность информационных систем и технологий в заданных функциональных характеристиках и соответствии критериям качества (ПК-30); способностью обеспечивать безопасность и целостность данных информационных систем и технологий (ПК-31); способностью адаптировать приложения к изменяющимся условиям функционирования (ПК-32).

4.2.Распределение формирования компетенций по дисциплинам модуля

Дисциплины модуля		ОПК-2	ПК-13	ПК-15	ПК-17	ПК-25	ПК-30	ПК-31	ПК-32
1	**(ВС)** *Безопасность баз данных*		+	+			+	+	+
2	**(ВС)** *Безопасность компьютерных сетей*		+	+	+		+	+	+
3	**(ВС)** *Криптографические методы защиты информации*	+				+	+	+	
4	**(ВС)** *Основы теории алгоритмов и анализа их сложности*	+			+	+		+	

5. ПРОМЕЖУТОЧНАЯ АТТЕСТАЦИЯ ПО МОДУЛЮ

5.1. Весовой коэффициент значимости промежуточной аттестации по модулю:

К = 0.4

5.2. Форма промежуточной аттестации по модулю:

Не предусмотрено

ПРИЛОЖЕНИЕ 1
к рабочей программе модуля

5.3. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО МОДУЛЮ

5.3.1. ОБЩИЕ КРИТЕРИИ ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО МОДУЛЮ

Система критериев оценивания результатов обучения в рамках модуля опирается на три уровня освоения: пороговый, повышенный, высокий.

Компоненты компетенций	**Признаки уровня освоения компонентов компетенций**		
	пороговый	**повышенный**	**высокий**
Знания	Студент демонстрирует знание-знакомство, знание-копию: узнает объекты, явления и понятия, находит в них различия, проявляет знание источников получения информации, может осуществлять самостоятельно репродуктивные действия над знаниями путем самостоятельного воспроизведения и применения информации.	Студент демонстрирует аналитические знания: уверенно воспроизводит и понимает полученные знания, относит их к той или иной классификационной группе, самостоятельно систематизирует их, устанавливает взаимосвязи между ними, продуктивно применяет в знакомых ситуациях.	Студент может самостоятельно извлекать новые знания из окружающего мира, творчески их использовать для принятия решений в новых и нестандартных ситуациях.
Умения	Студент умеет корректно выполнять предписанные действия по инструкции, алгоритму в известной ситуации, самостоятельно выполняет действия по решению типовых задач, требующих выбора из числа известных методов, в предсказуемо изменяющейся ситуации	Студент умеет самостоятельно выполнять действия (приемы, операции) по решению нестандартных задач, требующих выбора на основе комбинации известных методов, в непредсказуемо изменяющейся ситуации	Студент умеет самостоятельно выполнять действия, связанные с решением исследовательских задач, демонстрирует творческое использование умений (технологий)
Личностные качества	Студент имеет низкую мотивацию учебной деятельности, проявляет безразличное, безответственное отношение к учебе, порученному делу	Студент имеет выраженную мотивацию учебной деятельности, демонстрирует позитивное отношение к обучению и будущей трудовой деятельности, проявляет активность.	Студент имеет развитую мотивацию учебной и трудовой деятельности, проявляет настойчивость и увлеченность, трудолюбие, самостоятельность, творческий подход.

5.3.2. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО МОДУЛЮ

5.3.2.1. Перечень примерных вопросов для интегрированного экзамена по модулю

Не предусмотрено

5.3.2.2. Перечень примерных тем итоговых проектов по модулю.

Не предусмотрено

6. ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ В РАБОЧЕЙ ПРОГРАММЕ МОДУЛЯ

Номер листа изменений	Номер протокола заседания проектной группы модуля	Дата заседания проектной группы модуля	Всего листов в документе	Подпись руководителя проектной группы модуля

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«Уральский федеральный университет имени первого Президента России Б.Н. Ельцина»

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Безопасность баз данных

Перечень сведений о рабочей программе дисциплины	**Учетные данные**
Модуль *Методы защиты информационных технических систем*	**Код модуля** 1140368
Образовательная программа *Информационные системы в научно-технических и социально-экономических технологиях*	**Код ОП 09.03.02/01.01** **Учебный план № 5456**
Направление подготовки *Информационные системы и технологии*	**Код направления и уровня подготовки** *09.03.02*
Уровень подготовки *Бакалавр*	
ФГОС ВО	**Реквизиты приказа Минобрнауки РФ об утверждении ФГОС ВО**: *Приказ от 12.03.2015, №219*

Екатеринбург, 2018

Рабочая программа дисциплины составлена авторами:

№ п/п	ФИО	Ученая степень, ученое звание	Должность	Кафедра	Подпись
1	Субботин С.Г.		ст. препо-даватель	Технической физики	

Руководитель модуля К.В. Звонарев

Рекомендовано учебно-методическим советом института физико-технологического

Председатель учебно-методического совета В.В. Зверев
Протокол № _____ от _____ г.

Согласовано:

Дирекция образовательных программ Р.Х.Токарева

1. ОБЩАЯ ХАРАКТЕРИСТИКА ДИСЦИПЛИНЫ БЕЗОПАСНОСТЬ БАЗ ДАННЫХ

1.1.Аннотация содержания дисциплины

Дисциплина «Безопасность баз данных» относится к вариативной части образовательной программы (по выбору студента), входит в модуль «*Методы защиты информационных технических систем*». В процессе освоения дисциплины студентам предоставляется возможность получить комплексное всестороннее представление о работе с современными реляционными СУБД, обеспечения их безопасности, целостности и доступности, а также принципов проектирования баз данных. Изучаются различные методы обеспечения высокой доступности и отказоустойчивости – технология резервного копирования и восстановления данных, репликация данных, различные способы обеспечения аппаратной избыточности.

1.2. Язык реализации программы - русский

1.3. Планируемые результаты обучения по дисциплине

Результатом обучения в рамках дисциплины является формирование у студента следующих компетенций:

- способностью разрабатывать средства автоматизированного проектирования информационных технологий (ПК-13);
- способностью участвовать в работах по доводке и освоению информационных технологий в ходе внедрения и эксплуатации информационных систем (ПК-15);
- способностью поддерживать работоспособность информационных систем и технологий в заданных функциональных характеристиках и соответствии критериям качества (ПК-30);
- способностью обеспечивать безопасность и целостность данных информационных систем и технологий (ПК-31);
- способностью адаптировать приложения к изменяющимся условиям функционирования (ПК-32).

В результате освоения дисциплины студент должен:

Знать: принципы проектирования современных реляционных СУБД; основные элементы языка запросов SQL (в стандарте ANSI), типы данных ANSI SQL, а также объектные типы – XML, геометрические и географические данные; аппаратные и программные механизмы, обеспечивающие надежное хранение данных и устойчивость транзакций, основные проблемы, возникающие при многопользовательском доступе к данным, и способы их разрешения; основные принципы защиты данных – методы аутентификации в СУБД, ограничение доступа к данным, шифрование хранимых данных и сетевого трафика.

Уметь: создавать БД и структуры данных (таблицы, индексы) с учетом дополнительных требований по оптимизации скорости доступа; формировать SQL-запросы к СУБД.

Владеть навыками администрирования СУБД – конфигурировать службы СУБД, необходимые для работы, решать задачи резервного копирования и восстановления данных, вопросы ограничения доступа, автоматизировать управление СУБД; современными технологиями программирования приложений в части доступа к данным – ADO .NET, Entity Framework, LINQ to SQL, jDBC.

1.4. Объем дисциплины

№ п/п	Виды учебной работы	Объем дисциплины		Распределение объема дисциплины по семестрам (час.)
		Всего часов	В т.ч. контактная работа (час.)*	7 семестр
1.	**Аудиторные занятия**	**51**	**51**	**51**
2.	Лекции	34	34	34
3.	Практические занятия	-	-	-
4.	Лабораторные работы	17	17	17
5.	**Самостоятельная работа студентов, включая все виды текущей аттестации**	53	7.65	53
6.	**Промежуточная аттестация**	4	0,25	**Зачет, 4**
7.	**Общий объем по учебному плану, час.**	**108**	58,9	**108**
8.	**Общий объем по учебному плану, з.е.**	**3**	-	**3**

2. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Код раздела, темы	Раздел, тема дисциплины*	Содержание
Р1	Теоретические основы построения и эксплуатации баз данных	Определение СУБД. Первые СУБД, иерархическая и сетевая модели. Типовая блок-схема СУБД, описание принципов функционирования. Тенденции развития современных СУБД. Этапы проектирования базы данных. Элементы ER-модели. Бинарные и многосторонние связи. Подклассы. Представление ограничений в ER-модели. Принципы проектирования. Основные понятия – отношения, кортежи(записи), атрибуты. Преобразование ER-модели в реляционную схему, различные подходы. Функциональные зависимости, ключи отношений. Определение нормальных форм (1-4 НФ, НФ Бойса-Кодда). Декомпозиция, как способ устранения аномалий данных.
Р2	Язык запросов SQL.	Простые запросы на языке SQL. Проекция и выбор, операторы сравнения, сравнение со строками и значениями типа дата/время, значения NULL. Запросы к нескольким таблицам, виды соединений (JOIN). Подзапросы. Объединение, пересечение и разность запросов. Агрегирование данных и группировка. Модификация данных.

		Типы данных SQL. Объявление и модификация таблиц. Объявление индексов. Создание представлений (View). Ограничения (constraint) и триггеры. Объекты последовательного доступа к записям – курсоры (cursor). Реализация бизнес-логики – объявление хранимых процедур и функций.
Р3	Обеспечение целостности данных и отказоустойчивости.	Описание проблем, возникающих при конкурентном доступе к данным. Понятие транзакции, ее свойства. Обеспечение устойчивости транзакций, механизм блокирования и виды блокировок. Создание БД в среде MS SQL Server. Файлы базы данных. Оптимизация расположения файлов для ускорения доступа. Аппаратное обеспечение отказоустойчивости. Типы резервных копий и стратегии резервного копирования. Роль журнала транзакций. Восстановление данных из набора резервных копий, перенос файлов БД.
Р4	Управление доступом, вопросы безопасности.	Система аутентификации в MS SQL Server. Создание учетной записи, предоставление доступа к серверу и БД. Инструкции GRANT, REVOKE, DENY, настройка доступа к объектам сервера и БД, настройка прав на выполнение операций. Роли сервера и базы данных. Создание сертификатов и использование их для шифрования данных, использование протокола SSL для шифрования трафика.
Р5	Администрирование СУБД.	Подсистема репликации данных (на примере MS SQL Server), виды репликации. Механизм работы со связанными серверами (linked servers). Классификация задач обслуживания и управления. Утилита SQL Agent, задание расписаний и настройка оповещений. Утилита sqlcmd, реализация пакетных запросов. Планировщик Windows, реализация его помощью задач обслуживания. Массовая загрузка данных и программа bcp. Встроенные средства SQL Server – использование планов обслуживания (Maintenance Plans).

3. РАСПРЕДЕЛЕНИЕ УЧЕБНОГО ВРЕМЕНИ

3.1. Распределение аудиторной нагрузки и мероприятий самостоятельной работы по разделам дисциплины

Объем модуля (зач.ед.): 15
Объем дисциплины (зач.ед.): 3

Раздел дисциплины			Аудиторные занятия (час.)				Самостоятельная работа: виды, количество и объемы мероприятий																						
Код раздела, темы	Наименование раздела, темы	**Всего по разделу, теме (час.)**	**Всего аудиторной работы (час.)**	Лекции	Практические занятия	Лабораторные работы	**Всего самостоятельной работы студентов (час.)**	Подготовка к аудиторным занятиям (час.)					Выполнение самостоятельных внеаудиторных работ (колич.)											Подготовка к контрольным мероприятиям текущей аттестации (колич.)			Подготовка к промежуточной аттестации по дисциплине (час.)		Подготовка в рамках дисциплины к промежуточной аттестации по модулю (час.)	
								Всего (час.)	Лекция	Практ., семинар. занятие	Лабораторное занятие	Н/и семинар, семинар-конфер., коллоквиум (магистратура)	**Всего (час.)**	Домашняя работа*	Графическая работа*	Реферат, эссе, творч. работа*	Проектная работа*	Расчетная работа, разработка программного продукта*	Расчетно-графическая работа*	Домашняя работа на иностр. языке*	Перевод инояз. литературы*	Курсовая работа*	Курсовой проект*	**Всего (час.)**	Контрольная работа*	Коллоквиум*	Зачет	Экзамен	Интегрированный экзамен по модулю	Проект по модулю
Р1	Теоретические основы построения и эксплуатации баз данных	22	10	10			12	10	10															2	1					
Р2	Язык запросов SQL	24	12	8		4	12	12	8		4																			
Р3	Обеспечение целостности данных и отказоустойчивости	24	12	8		4	12	12	8		4																			
Р4	Управление доступом, вопросы безопасности	16	8	4		4	8	8	4		4																			
Р5	Администрирование СУБД	18	9	4		5	9	9	4		5																			
	Всего (час), без учета промежуточной аттестации**:**	**104**	**51**	**34**	**0**	**17**	**53**	**51**	**34**	**0**	**17**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**2**	**2**					
	Всего по дисциплине (час.):	**108**	**51**				**57**	В т.ч. промежуточная аттестация																			4	0	**0**	0

4. ОРГАНИЗАЦИЯ ПРАКТИЧЕСКИХ ЗАНЯТИЙ, САМОСТОЯТЕЛЬНОЙ РАБОТЫ ПО ДИСЦИПЛИНЕ

4.1. Лабораторные работы

Код раздела, темы	Номер работы	Наименование работы	Время на выполнение работы (час.)
Р2	1	Проектирование баз данных средствами SQL Server Management Studio	1
Р2	2	Реализация запросов SELECT	2
Р2	3	Работа с бинарными объектами в SQL, хранение документов в столбцах VARBINARY(MAX)	2
Р2	4	Создание объектов БД (уровень схемы данных)	2
Р3	5	Практическое использование транзакций. Уровни изоляции транзакций.	2
Р3	6	Создание, изменение и удаление баз данных. Реализация схемы секционирования.	2
Р3	7	Резервное копирование и восстановление БД.	2
Р4	8	Управление доступом - создание учетных записей SQL сервера, пользователей БД, работа с ролями сервера и БД, назначение прав (GRANT|REVOKE|DENY). Управление сертификатами.	2
Р5	9	Настройка репликации транзакций. Задачи администрирования	2
		Всего:	17

4.2. Практические занятия

не предусмотрено

4.3.Примерная тематика самостоятельной работы

4.3.1. Примерный перечень тем домашних работ

не предусмотрено

4.3.2. Примерный перечень тем графических работ

не предусмотрено

4.3.3. Примерный перечень тем рефератов (эссе, творческих работ)

не предусмотрено

4.3.4 Примерная тематика индивидуальных или групповых проектов

не предусмотрено

4.3.5. Примерный перечень тем расчетных работ (программных продуктов)

не предусмотрено

4.3.6. Примерный перечень тем расчетно-графических работ

не предусмотрено

4.3.7. Примерный перечень тем курсовых проектов (курсовых работ)

не предусмотрено

4.3.8. Примерная тематика контрольных работ

- ER-модель. Терминология и применение
- Язык SQL. Запросы SELECT и создание объектов БД

4.3.9. Примерная тематика коллоквиумов

не предусмотрено

5. СООТНОШЕНИЕ РАЗДЕЛОВ, ТЕМ ДИСЦИПЛИНЫ И ПРИМЕНЯЕМЫХ ТЕХНОЛОГИЙ ОБУЧЕНИЯ

Код раздела, темы дисциплины	Активные методы обучения						Дистанционные образовательные технологии и электронное обучение					
	Проектная работа	Кейс-анализ	Деловые игры	Проблемное обучение	Командная работа	Другие (диалоговое обсуждение пройденного)	Сетевые учебные курсы	Виртуальные практикумы и тренажеры	Вебинары и видеоконференции	Асинхронные web-конференции и семинары	Совместная работа и разработка контента	Другие (указать, какие)
P1-P5				*	*							

6. ПРОЦЕДУРЫ КОНТРОЛЯ И ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ (Приложение 1)

7. ПРОЦЕДУРЫ ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ В РАМКАХ НЕЗАВИСИМОГО ТЕСТОВОГО КОНТРОЛЯ (Приложение 2)

8. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ (Приложение 3)

9. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

9.1.Рекомендуемая литература

9.1.1.Основная литература

1. СУБД: язык SQL в примерах и задачах [Электронный ресурс] : учеб. пособие / И.Ф. Астахова [и др.]. — Электрон. дан. — Москва : Физматлит, 2009. — 168 с. — Режим доступа: https://e.lanbook.com/book/2101
2. Бурков, А.В. Проектирование информационных систем в Microsoft SQL Server 2008 и Visual Studio 2008 / А.В. Бурков. - М. : Интернет-Университет Информационных Технологий, 2010. - 273 с. ; То же [Электронный ресурс]. - URL: //biblioclub.ru/index.php?page=book&id=233750.
3. Маркин А.В. Построение запросов и программирование на SQL: учебное пособие, Диалог-МИФИ, 2014. - 384 с.; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book_view_red&book_id=89077

9.1.2. Дополнительная литература

1. Кузнецов С. Введение в модель данных SQL: курс, Национальный Открытый Университет «ИНТУИТ», 2016. – 351 с.; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book_view_red&book_id=429087
2. Дьяков И.А. Базы данных. Язык SQL: учебное пособие, Издательство ФГБОУ ВПО «ТГТУ», 2012. – 82 с.; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book_view_red&book_id=277628
3. Кара-Ушанов, В.Ю. SQL — язык реляционных баз данных: учебное пособие [Электронный ресурс] — Электрон. дан. — Екатеринбург : УрФУ, 2016. — 156 с. — Режим доступа: https://e.lanbook.com/book/98296.
4. Гуляев В.Д. Структура языка SQL Лаборатория книги, 2012. – 93 с.; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book_view_red&book_id=142513
5. Полякова Л.Н. Основы SQL, Интернет-Университет Информационных Технологий, 2004. – 368 с.; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book_view_red&book_id=233205

9.2.Методические разработки

не используются.

9.3.Программное обеспечение

Windows 2008 Server, MS SQL Server 2012.

9.4. Базы данных, информационно-справочные и поисковые системы

1. Государственная публичная научно-техническая библиотека: http://www/gpntb.ru
2. Библиотека УрФУ: http://lib.urfu.ru

9.5.Электронные образовательные ресурсы

не используются

10. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Сведения об оснащенности дисциплины специализированным и лабораторным оборудованием

Лекции и лабораторные работы проводятся в аудитории, оснащенной проектором с использованием мобильного компьютера (ноутбука). Компьютерный класс с установленным программным обеспечением п.9.3 и числом рабочих мест соответствующим числу студентов в группе. Допустимо один компьютер на двух обучающихся.

ПРИЛОЖЕНИЕ 1
к рабочей программе дисциплины

6. ПРОЦЕДУРЫ КОНТРОЛЯ И ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ В РАМКАХ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ

6.1. Весовой коэффициент значимости дисциплины – 1

6.2.Процедуры текущей и промежуточной аттестации по дисциплине

1.Лекции: коэффициент значимости совокупных результатов лекционных занятий – 0,5

Текущая аттестация на лекциях	**Сроки – семестр, учебная неделя**	**Максимальная оценка в баллах**
Посещение лекций	7 семестр, 1 – 18 учебные недели	50
Контрольная работа	7 семестр, 8 – 9 учебные недели	50
Весовой коэффициент значимости результатов текущей аттестации по лекциям – 0,4		
Промежуточная аттестация по лекциям – зачет **Весовой коэффициент значимости результатов промежуточной аттестации по лекциям – 0,6**		
2. Лабораторные занятия: коэффициент значимости совокупных результатов лабораторных занятий – 0,5		
Текущая аттестация на лабораторных занятиях	**Сроки – семестр, учебная неделя**	**Максимальная оценка в баллах**
Посещение лабораторных занятий	7 семестр, 10-18 учебная неделя	100
Весовой коэффициент значимости результатов текущей аттестации по лабораторным занятиям - 1		
Промежуточная аттестация по лабораторным занятиям– нет **Весовой коэффициент значимости результатов промежуточной аттестации по лабораторным занятиям– 0**		

6.3. Процедуры текущей и промежуточной аттестации курсовой работы/проекта
Не предусмотрено

6.4. Коэффициент значимости семестровых результатов освоения дисциплины
Не предусмотрено

ПРИЛОЖЕНИЕ 2
к рабочей программе дисциплины

7. ПРОЦЕДУРЫ ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ В РАМКАХ НЕЗАВИСИМОГО ТЕСТОВОГО КОНТРОЛЯ

Дисциплина и ее аналоги, по которым возможно тестирование, отсутствуют на сайте ФЭПО http://fepo.i-exam.ru.

Дисциплина и ее аналоги, по которым возможно тестирование, отсутствуют на сайте Интернет-тренажеры http://training.i-exam.ru.

Дисциплина и ее аналоги, по которым возможно тестирование, отсутствуют на портале СМУДС УрФУ.

В связи с отсутствием Дисциплины и ее аналогов, по которым возможно тестирование, на сайтах ФЭПО, Интернет-тренажеры и портале СМУДС УрФУ, тестирование в рамках НТК не проводится.

ПРИЛОЖЕНИЕ 3
к рабочей программе дисциплины

8. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ

8.1. КРИТЕРИИ ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ КОНТРОЛЬНО-ОЦЕНОЧНЫХ МЕРОПРИЯТИЙ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ В РАМКАХ БРС

В рамках БРС применяются утвержденные на кафедре критерии оценивания достижений студентов по каждому контрольно-оценочному мероприятию. Система критериев оценивания, как и при проведении промежуточной аттестации по модулю, опирается на три уровня освоения компонентов компетенций: пороговый, повышенный, высокий.

Компоненты компетенций	**Признаки уровня освоения компонентов компетенций**		
	пороговый	**повышенный**	**высокий**
Знания	Студент демонстрирует знание-знакомство, знание-копию: узнает объекты, явления и понятия, находит в них различия, проявляет знание источников получения информации, может осуществлять самостоятельно репродуктивные действия над знаниями путем самостоятельного воспроизведения и применения информации.	Студент демонстрирует аналитические знания: уверенно воспроизводит и понимает полученные знания, относит их к той или иной классификационной группе, самостоятельно систематизирует их, устанавливает взаимосвязи между ними, продуктивно применяет в знакомых ситуациях.	Студент может самостоятельно извлекать новые знания из окружающего мира, творчески их использовать для принятия решений в новых и нестандартных ситуациях.
Умения	Студент умеет корректно выполнять предписанные действия по инструкции, алгоритму в известной ситуации, самостоятельно выполняет действия по решению типовых задач, требующих выбора из числа известных методов, в предсказуемо изменяющейся ситуации	Студент умеет самостоятельно выполнять действия (приемы, операции) по решению нестандартных задач, требующих выбора на основе комбинации известных методов, в непредсказуемо изменяющейся ситуации	Студент умеет самостоятельно выполнять действия, связанные с решением исследовательских задач, демонстрирует творческое использование умений (технологий)
Личностные качества	Студент имеет низкую мотивацию учебной деятельности, проявляет безразличное, безответственное отношение к учебе, порученному делу	Студент имеет выраженную мотивацию учебной деятельности, демонстрирует позитивное отношение к обучению и будущей трудовой деятельности, проявляет активность.	Студент имеет развитую мотивацию учебной и трудовой деятельности, проявляет настойчивость и увлеченность, трудолюбие, самостоятельность, творческий подход.

8.2. КРИТЕРИИ ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПРИ ИСПОЛЬЗОВАНИИ НЕЗАВИСИМОГО ТЕСТОВОГО КОНТРОЛЯ

При проведении независимого тестового контроля как формы промежуточной аттестации применяется методика оценивания результатов, предлагаемая разработчиками тестов. Процентные показатели результатов независимого тестового контроля переводятся в баллы промежуточной аттестации по 100-балльной шкале в БРС:

- в случае балльной оценки по тесту (блокам, частям теста) переводится процент набранных баллов от общего числа возможных баллов по тесту;
- при отсутствии балльной оценки по тесту переводится процент верно выполненных заданий теста, от общего числа заданий.

8.3. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

8.3.1. Примерные задания для проведения мини-контрольных в рамках учебных занятий

не предусмотрено

8.3.2. Примерные контрольные задачи в рамках учебных занятий

Задание: для заданной в варианте предметной области спроектировать базу данных. Создать спроектированную базу с использованием СУБД MSSQL. Реализовать приложение, взаимодействующее с базой данных, и позволяющее выполнять просмотр, добавление и удаления данных в БД.

Вариант 1

База данных хранит данные об организациях некоторого города. Каждая организация относится к одной или нескольким сферам деятельности. Для каждой организации задаются как минимум почтовый индекс, район города, адрес, любое количество телефонов, адрес сайта, любое количество адресов электронной почты, время работы.

Приложение позволяет искать в базе данных организации по заданным названию, району, адресу, номеру телефона или адресу сайта.

Вариант 2

База данных хранит данные об имеющихся в домашней библиотеке книгах. У каждой книги может быть несколько авторов, она может быть издана одновременно несколькими издательствами, может относиться к нескольким жанрам. Для каждой книги хранятся число страниц, год издания, место издания, шифр ISBN, тип переплёта.

Приложение позволяет искать в базе данных книги по заданным названию, автору, жанру, году издания или издательству.

Вариант 3

База данных хранит данные о модельном ряде некоторого производителя автомобилей. Для каждой модели хранится класс автомобиля (например, «эконом-класс», «бизнес-класс»), тип кузова, количество мест и дверей, тип КПП, название модели двигателя, объём и мощность двигателя, средний расход топлива, максимальная скорость, цена. Одна и та же модель двигателя может устанавливаться на различные модели автомобилей.

Приложение позволяет искать в базе данных модели автомобилей по заданным классу автомобиля, типу кузова, типу АКПП, расходу топлива или цене.

Вариант 4

База данных хранит результаты финальных матчей всех чемпионатов мира по футболу. Для каждого матча хранятся названия стран-участниц финального матча, счёт, забитые в матче голы, фамилии тренеров, год и место (страна, город) проведения чемпионата мира. Для каждого гола хранится автор гола, минута, на которой он был забит, тип гола (с игры, с пенальти или в свои ворота). Один и тот же тренер или игрок могли принимать участие в разных финальных матчах.

Приложение позволяет искать в базе данных:
всех чемпионов мира и всех финалистов с указанием, сколько раз они становились чемпионами или финалистами;
количество голов, которые забил во всех финальных матчах заданный футболист; сколько раз сборная заданной страны или тренер становились чемпионом мира; все данные о финальном матче чемпионата мира, проходившего в заданный год.

Вариант 5

База данных хранит данные об имеющихся в домашней аптечке лекарствах. Для каждого препарата хранится его латинское название, фирма-производитель, дата изготовления, срок годности, тип лекарства (капли, таблетки, спрей, …), количество упаковок, заболевания, для которых оно применяется. Каждое заболевание относится к какой-либо группе заболеваний.

Приложение позволяет искать в базе данных лекарства по заданным названию, типу лекарства, заболеванию или группе заболеваний, а также искать по этим критериям только среди тех лекарств, которые являются не просроченными на заданную дату.

Вариант 5

База данных хранит данные о работающих в организации сотрудниках. Для каждого сотрудника хранятся фамилия, имя, отчество, дата рождения, пол, номер и серия паспорта, должность, вид образования (среднее, высшее, …), специальность, зарплата, дата приёма на работу. Один и тот же сотрудник может иметь несколько специальностей и занимать несколько должностей.

Приложение позволяет искать в базе данных сотрудников по заданным фамилии, полу, должности, специальности, виду образования или зарплате.

Вариант 7

База данных хранит географические сведения о разных странах. Для каждой страны хранятся столица, площадь, число жителей, национальности жителей, расположенные на территории страны реки, горы, озёра. Для каждой реки задаётся её длина, для каждой горы – её высота, для каждого озера – его площадь. В одной стране могут проживать люди разных национальностей, для каждой национальности, проживающей в заданной стране, хранится численность народа. Также в каждой стране может быть расположено несколько гор, рек, озёр.

Приложение позволяет искать в базе данных:
самую высокую горную вершину и суммарные протяжённость рек и площадь озёр в заданной стране; в каких странах расположена заданная река, гора или озеро; сколько и в каких странах проживают жители заданной национальности; всю хранящуюся в базе информацию о заданной стране.

Вариант 8

База данных хранит данные о лауреатах Нобелевской премии. Для каждого лауреата хранятся фамилия, имя, отчество, страна, год получения Нобелевской премии, область науки, описание открытия. Нобелевская премия в одном году по одной области науки может быть присуждена нескольким учёным.

Приложение позволяет искать в базе данных лауреатов премии по заданным году, области науки, части описания открытия или стране, а также строить список стран с указанием количества представляющих страну лауреатов по заданной области науки.

Вариант 9

База данных хранит данные о модельном ряде некоторого производителя ноутбуков. Для каждой модели хранится название модели ноутбука, название модели процессора, размер экрана, размеры и типы оперативной памяти и жёсткого диска, модель видеокарты, вес, цена. Одна и та же модель процессора и видеокарты может устанавливаться на различные модели ноутбуков. Модель процессора характеризуется названием, тактовой частотой, количеством ядер, размером кэш-памяти. Модель видеокарты характеризуется названием, максимальным разрешением, частотой, размером встроенной памяти.

Приложение позволяет искать в базе данных модели ноутбуков по заданным размеру экрана, тактовой частоте процессора, объёму оперативной памяти и жёсткого диска, весу или цене.

Вариант 10

База данных хранит данные о закончивших некоторый факультет студентах. Для каждого студента хранится фамилия, имя, отчество, пол, курс, группа, список сданных экзаменов и зачётов с указанием семестра, в котором они сдавались, названия дисциплины, оценки, даты сдачи и принимавшего экзамен или зачёт преподавателя. Каждый экзамен или зачёт мог сдаваться несколько раз (в этом случае нужно хранить все оценки и даты пересдач), по некоторым дисциплинам было несколько экзаменов или зачётов. Все дисциплины делятся на естественно-научные, гуманитарно-экономические и специализированные циклы.
Приложение позволяет искать в базе данных:
результаты сдачи заданной сессии выбранным студентом; средний балл всех студентов по всем дисциплинам или по выбранному циклу дисциплин;
результаты (дата, оценка, количество попыток) сдачи заданного экзамена или зачёта всеми студентами; итоговые оценки за все экзамены и зачёты выбранного студента с указанием преподавателей, их поставивших.

8.3.3. Примерные контрольные кейсы

не предусмотрено

8.3.4. Перечень примерных вопросов для зачета

- Определение СУБД. Описание основных структурных частей.
- ER-модель. Графическое представление
- Основные положения реляционной модели данных
- Реляционная модель. Функциональные зависимости, определение ключа и суперключа.
- Реляционная модель. Определение нормальных форм. Декомпозиция
- Запросы SELECT. Выборка и фильтрация данных, запросы к нескольким отношениям (таблицам БД), агрегирование и группировка данных.
- Язык описания метаданных DDL. Создание и изменение объектов БД
- Определение и свойства транзакций. Уровни изоляции транзакций. Операции ROLLBACK и ROLLFORWARD при перезагрузке SQL сервера. Роль журнала транзакций, определение контрольной точки
- Создание БД. Перечень файлов, из которых состоит БД, их назначение. Пример инструкции по созданию, объяснение основных параметров
- Стратегии резервного копирования БД, перечень и особенности. Выбор стратегии
- Способы восстановления БД. Получение информации о наборе резервных копий. Перенос файлов базы данных
- Подсистема аутентификации SQL Server. Создание учетных записей сервера и пользователей БД. Назначение полномочий, примеры Grant|Revoke|Deny. Роли сервера и БД.
- Управление сертификатами и асимметричными ключами, их применение для шифрования данных.
- Понятие репликации, описание различных типов репликации.
- Классификация задач администратора СУБД.
- Консольные утилиты для доступа к MS SQL Server, перечень и использование.

8.3.5. Перечень примерных вопросов для экзамена

не предусмотрен

8.3.6. Ресурсы АПИМ УрФУ, СКУД УрФУ для проведения тестового контроля в рамках текущей и промежуточной аттестации

не используются

8.3.7. Ресурсы ФЭПО для проведения независимого тестового контроля

не используются

8.3.8. Интернет-тренажеры

не используются

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«Уральский федеральный университет имени первого Президента России Б.Н. Ельцина»

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Безопасность компьютерных сетей

Перечень сведений о рабочей программе дисциплины	**Учетные данные**
Модуль *Методы защиты информационных технических систем*	**Код модуля** 1140368
Образовательная программа *Информационные системы в научно-технических и социально-экономических технологиях*	**Код ОП 09.03.02/01.01** **Учебный план № 5456**
Направление подготовки *Информационные системы и технологии*	**Код направления и уровня подготовки** *09.03.02*
Уровень подготовки *Бакалавр*	
ФГОС ВО	**Реквизиты приказа Минобрнауки РФ об утверждении ФГОС ВО**: *Приказ от 12.03.2015, №219*

Екатеринбург, 2018

Рабочая программа дисциплины составлена авторами:

№ п/п	ФИО	Ученая степень, ученое звание	Должность	Кафедра	Подпись
1	Звонарев К.В.	к.ф.-м.н.	доцент	Технической физики	

Руководитель модуля К.В. Звонарев

Рекомендовано учебно-методическим советом института физико-технологического

Председатель учебно-методического совета В.В. Зверев
Протокол № _____ от _____ г.

Согласовано:

Дирекция образовательных программ Р.Х.Токарева

1. ОБЩАЯ ХАРАКТЕРИСТИКА ДИСЦИПЛИНЫ БЕЗОПАСНОСТЬ КОМПЬЮТЕРНЫХ СЕТЕЙ

1.1.Аннотация содержания дисциплины

Дисциплина «Безопасность компьютерных сетей» относится к вариативной части образовательной программы (по выбору студента), входит в модуль «*Методы защиты информационных технических систем*». В процессе освоения дисциплины студентам предоставляется возможность получить комплексное всестороннее представление о принципах построения систем защиты информации в компьютерных сетях. Рассматриваются подсистемы аутентификации и разграничения доступа в вычислительных сетях, безопасность сетевых протоколов, различные виды сетевых атак и средства защиты от них. Студенты получают практические навыки работы с различным ПО, предназначенным для исследования сетей на уязвимости, а также противодействия сетевым атакам.

1.2. Язык реализации программы - русский

1.3. Планируемые результаты обучения по дисциплине

Результатом обучения в рамках дисциплины является формирование у студента следующих компетенций:

- способностью разрабатывать средства автоматизированного проектирования информационных технологий (ПК-13);
- способностью участвовать в работах по доводке и освоению информационных технологий в ходе внедрения и эксплуатации информационных систем (ПК-15);
- способностью использовать технологии разработки объектов профессиональной деятельности в областях: безопасность информационных систем, управление технологическими процессами, техническая физика, энергетика, ядерная энергетика, в условиях экономики информационного общества (ПК-17);
- способностью поддерживать работоспособность информационных систем и технологий в заданных функциональных характеристиках и соответствии критериям качества (ПК-30);
- способностью обеспечивать безопасность и целостность данных информационных систем и технологий (ПК-31);
- способностью адаптировать приложения к изменяющимся условиям функционирования (ПК-32).

В результате освоения дисциплины студент должен:

Знать: принципы построения подсистем защиты в компьютерных сетях различной архитектуры; основы функционирования современных систем идентификации и аутентификации; средства и методы реализации атак на сетевые ресурсы, принципы использования межсетевых экранов и построения виртуальных частных сетей;

Уметь: оценивать эффективность и надежность защиты компьютерной сети; выявлять слабости защиты вычислительной сети и использовать их для вскрытия защиты;

Владеть: навыками администрирования современных компьютерных сетей; навыками использования межсетевых экранов, сканеров уязвимостей и систем обнаружения вторжений.

1.4. Объем дисциплины

№ п/п	Виды учебной работы	Объем дисциплины		Распределение объема дисциплины по семестрам (час.)
		Всего часов	В т.ч. контактная работа (час.)*	8 семестр
1.	**Аудиторные занятия**	**48**	**48**	**48**
2.	Лекции	16	16	16
3.	Практические занятия	-	-	-
4.	Лабораторные работы	32	32	32
5.	**Самостоятельная работа студентов, включая все виды текущей аттестации**	56	7,2	56
6.	**Промежуточная аттестация**	4	0,25	**Зачет, 4**
7.	**Общий объем по учебному плану, час.**	**108**	55,45	**108**
8.	**Общий объем по учебному плану, з.е.**	**3**	-	**3**

2. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Код раздела, темы	Раздел, тема дисциплины*	Содержание
Р1	Введение	Основные понятия и определения из области информационной безопасности. Средства и методы защиты информации в компьютерных сетях.
Р2	Процедуры локальной и сетевой аутентификации и авторизации	Основные средства и методы аутентификации в компьютерных системах. Способы хранения паролей пользователей. Удаленная аутентификация с помощью протоколов CHAP, MS-CHAP, S-KEY, Kerberos.
Р3	Безопасность стека протоколов TCP/IP. Сетевые атаки.	Семиуровневая модель OSI. Инкапсуляция и демультиплексирование сетевых пакетов. Безопасность основных сетевых протоколов ARP, IP, TCP, UDP, ICMP. Способы и средства реализации сетевых атак с использованием уязвимостей стека протоколов TCP/IP.
Р4	Обеспечение безопасности сетей с использованием протоколов защиты сетевого трафика	Безопасность удаленного терминала – протокол SSH. Межсетевые и экраны и трансляция сетевых адресов. Виртуальные частные сети. Протокол IPSec.
Р5	Сканирование сетей на уязвимости и системы обнаружения вторжений	Сканер портов Nmap. Сканер уязвимостей Nessus. Сеть ориентированные и хост ориентированные системы обнаружения вторжения. Система обнаружения вторжения Snort.

3. РАСПРЕДЕЛЕНИЕ УЧЕБНОГО ВРЕМЕНИ

3.1. Распределение аудиторной нагрузки и мероприятий самостоятельной работы по разделам дисциплины

Объем модуля (зач.ед.): 15
Объем дисциплины (зач.ед.): 3

Раздел дисциплины			Аудиторные занятия (час.)				Самостоятельная работа: виды, количество и объемы мероприятий																						
Код раздела, темы	Наименование раздела, темы	**Всего по разделу, теме (час.)**	**Всего аудиторной работы (час.)**	Лекции	Практические занятия	Лабораторные работы	**Всего самостоятельной работы студентов (час.)**	Подготовка к аудиторным занятиям (час.)					Выполнение самостоятельных внеаудиторных работ (колич.)											Подготовка к контрольным мероприятиям текущей аттестации (колич.)			Подготовка к промежуточной аттестации по дисциплине (час.)		Подготовка в рамках дисциплины к промежуточной аттестации по модулю (час.)	
								Всего (час.)	Лекция	Практ., семинар. занятие	Лабораторное занятие	Н/и семинар, семинар-конфер., коллоквиум (магистратура)	**Всего (час.)**	Домашняя работа*	Графическая работа*	Реферат, эссе, творч. работа*	Проектная работа*	Расчетная работа, разработка программного продукта*	Расчетно-графическая работа*	Домашняя работа на иностр. языке*	Перевод иноя3. литературы*	Курсовая работа*	Курсовой проект*	**Всего (час.)**	Контрольная работа*	Коллоквиум*	Зачет	Экзамен	Интегрированный экзамен по модулю	Проект по модулю
Р1	Введение	4	2	2			2	2	2																					
Р2	Процедуры локальной и сетевой аутентификации и авторизации	14	6	2		4	8	6	2		4													2	1					
Р3	Безопасность стека протоколов TCP/IP. Сетевые атаки.	16	8	4		4	8	8	4		4																			
Р4	Обеспечение безопасности сетей с использованием протоколов защиты сетевого трафика	30	18	4		14	19	19	4		15																			
Р5	Сканирование сетей на уязвимости и системы обнаружения вторжений	26	14	4		10	19	19	4		15																			
	Всего (час), без учета промежуточной аттестации:	**90**	**48**	**16**	**0**	**32**	**56**	**54**	**16**	**0**	**38**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**2**	**2**					
	Всего по дисциплине (час.):	**108**	**48**				**60**	В т.ч. промежуточная аттестация																			4	0	**0**	0

4. ОРГАНИЗАЦИЯ ПРАКТИЧЕСКИХ ЗАНЯТИЙ, САМОСТОЯТЕЛЬНОЙ РАБОТЫ ПО ДИСЦИПЛИНЕ

4.1. Лабораторные работы

Код раздела, темы	Номер работы	Наименование работы	Время на выполнение работы (час.)
Р2	1-2	Подсистема разграничения доступа в ОС UNIX. Защита сетевых сервисов	4
Р3	3-4	Основы межсетевого взаимодействия. Исследование безопасности основных протоколов с помощью утилиты tcpdump.	4
Р4	5	Защита сетевого соединения с помощью протокола SSH	2
Р4	6-8	Настройка межсетевого экрана и трансляции адресов в ОС FreeBSD	6
Р4	9-11	Организация VPN на базе протокола IPSec	6
Р5	12-14	Сканирование сетей на уязвимости с использованием сканер портов Nmap и сканера уязвимостей Nessus.	6
Р5	15-16	Работа с системой обнаружения вторжений Snort	4
		Всего:	32

4.2. Практические занятия

не предусмотрено

4.3.Примерная тематика самостоятельной работы

4.3.1. Примерный перечень тем домашних работ

не предусмотрено

4.3.2. Примерный перечень тем графических работ

не предусмотрено

4.3.3. Примерный перечень тем рефератов (эссе, творческих работ)

не предусмотрено

4.3.4 Примерная тематика индивидуальных или групповых проектов

не предусмотрено

4.3.5. Примерный перечень тем расчетных работ (программных продуктов)

не предусмотрено

4.3.6. Примерный перечень тем расчетно-графических работ

не предусмотрено

4.3.7. Примерный перечень тем курсовых проектов (курсовых работ)

не предусмотрено

4.3.8. Примерная тематика контрольных работ

- Основные виды подсистем аутентификации.
- Вычисление хешей в операционных системах и способы хранения паролей.
- Протоколы удаленной аутентификации.
- Трех сторонняя аутентификация в протоколе Kerberos

4.3.9. Примерная тематика коллоквиумов

не предусмотрено

5. СООТНОШЕНИЕ РАЗДЕЛОВ, ТЕМ ДИСЦИПЛИНЫ И ПРИМЕНЯЕМЫХ ТЕХНОЛОГИЙ ОБУЧЕНИЯ

Код раздела, темы дисциплины	Активные методы обучения						Дистанционные образовательные технологии и электронное обучение					
	Проектная работа	Кейс-анализ	Деловые игры	Проблемное обучение	Командная работа	Другие (диалоговое обсуждение пройденного)	Сетевые учебные курсы	Виртуальные практикумы и тренажеры	Вебинары и видеоконференции	Асинхронные web-конференции и семинары	Совместная работа и разработка контента	Другие (указать, какие)
Р1-Р5				*	*							

6. ПРОЦЕДУРЫ КОНТРОЛЯ И ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ (Приложение 1)

7. ПРОЦЕДУРЫ ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ В РАМКАХ НЕЗАВИСИМОГО ТЕСТОВОГО КОНТРОЛЯ (Приложение 2)

8. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ (Приложение 3)

9. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

9.1.Рекомендуемая литература

9.1.1.Основная литература

1. Мэйволд, Э. Безопасность сетей / Э. Мэйволд. - 2-е изд., испр. - М. : Национальный Открытый Университет «ИНТУИТ», 2016. - 572 с. : схем., ил. ; То же [Электронный ресурс]. - URL: //biblioclub.ru/index.php?page=book&id=429035.
2. Технологии защиты информации в компьютерных сетях / Н.А. Руденков, А.В. Пролетарский, Е.В. Смирнова, А.М. Суровов. - 2-е изд., испр. - М. : Национальный Открытый Университет «ИНТУИТ», 2016. - 369 с. : ил. ; То же [Электронный ресурс]. - URL: //biblioclub.ru/index.php?page=book&id=428820.
3. Прохорова, О.В. Информационная безопасность и защита информации : учебник / О.В. Прохорова ; Министерство образования и науки РФ, Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Самарский государственный архитектурно-строительный университет». - Самара : Самарский государственный архитектурно-строительный университет, 2014. - 113 с.; То же [Электронный ресурс]. - URL: //biblioclub.ru/index.php?page=book&id=438331.

9.1.2. Дополнительная литература

1. Голиков А.М. Защита информации в инфокоммуникационных системах и сетях: учебное пособие, Томский государственный университет систем управления и радиоэлектроники, 2015.

- 284 с.; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book_view_red&book_id=480637
2. Кияев В., Граничин О. Безопасность информационных систем: курс, Национальный Открытый Университет «ИНТУИТ», 2016. - 192 с.; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book_view_red&book_id=429032

9.2.Методические разработки

1. Синадский Н. И. Защита информации в компьютерных сетях: учебное пособие – Екатеринбург: УрГУ, 2008. – 225 с.
2. Синадский Н.И., Соболев О.Н. Угрозы безопасности компьютерной информации: Учеб. пособие. — Екатеринбург: Изд-во Урал. ун-та, 2000. — 85 с.

9.3.Программное обеспечение

Windows 2003 Server, FreeBSD, Nmap, Nessus, Snort.

9.4. Базы данных, информационно-справочные и поисковые системы

1. Государственная публичная научно-техническая библиотека: http://www/gpntb.ru
2. Библиотека УрФУ: http://lib.urfu.ru

9.5.Электронные образовательные ресурсы

Портал http://study.urfu.ru/ (Ресурс №8239).

10. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Сведения об оснащенности дисциплины специализированным и лабораторным оборудованием

Лекции и лабораторные работы проводятся в аудитории, оснащенной проектором с использованием мобильного компьютера (ноутбука). Компьютерный класс с установленным программным обеспечением п.9.3 и числом рабочих мест соответствующим числу студентов в группе. Допустимо один компьютер на двух обучающихся.

ПРИЛОЖЕНИЕ 1
к рабочей программе дисциплины

6. ПРОЦЕДУРЫ КОНТРОЛЯ И ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ В РАМКАХ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ

6.1. Весовой коэффициент значимости дисциплины – 1

6.2.Процедуры текущей и промежуточной аттестации по дисциплине

1.Лекции: коэффициент значимости совокупных результатов лекционных занятий – 0,5		
Текущая аттестация на лекциях	**Сроки – семестр, учебная неделя**	**Максимальная оценка в баллах**
Посещение лекций	8 семестр, 1 – 9 учебные недели	50
Контрольная работа	8 семестр, 8 – 9 учебные недели	50

Весовой коэффициент значимости результатов текущей аттестации по лекциям – 0,4		
Промежуточная аттестация по лекциям – зачет **Весовой коэффициент значимости результатов промежуточной аттестации по лекциям – 0,6**		
2. Лабораторные занятия: коэффициент значимости совокупных результатов лабораторных занятий – 0,5		
Текущая аттестация на лабораторных занятиях	**Сроки – семестр, учебная неделя**	**Максимальная оценка в баллах**
Посещение лабораторных занятий	7 семестр, 1-18 учебная неделя	100
Весовой коэффициент значимости результатов текущей аттестации по лабораторным занятиям - 1		
Промежуточная аттестация по лабораторным занятиям – нет **Весовой коэффициент значимости результатов промежуточной аттестации по лабораторным занятиям– 0**		

6.3. Процедуры текущей и промежуточной аттестации курсовой работы/проекта
Не предусмотрено

6.4. Коэффициент значимости семестровых результатов освоения дисциплины
Не предусмотрено

ПРИЛОЖЕНИЕ 2
к рабочей программе дисциплины

7. ПРОЦЕДУРЫ ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ В РАМКАХ НЕЗАВИСИМОГО ТЕСТОВОГО КОНТРОЛЯ

Дисциплина и ее аналоги, по которым возможно тестирование, отсутствуют на сайте ФЭПО http://fepo.i-exam.ru.

Дисциплина и ее аналоги, по которым возможно тестирование, отсутствуют на сайте Интернет-тренажеры http://training.i-exam.ru.

Дисциплина и ее аналоги, по которым возможно тестирование, отсутствуют на портале СМУДС УрФУ.

В связи с отсутствием Дисциплины и ее аналогов, по которым возможно тестирование, на сайтах ФЭПО, Интернет-тренажеры и портале СМУДС УрФУ, тестирование в рамках НТК не проводится.

ПРИЛОЖЕНИЕ 3
к рабочей программе дисциплины

8. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ

8.1. КРИТЕРИИ ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ КОНТРОЛЬНО-ОЦЕНОЧНЫХ МЕРОПРИЯТИЙ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ В РАМКАХ БРС

В рамках БРС применяются утвержденные на кафедре критерии оценивания достижений студентов по каждому контрольно-оценочному мероприятию. Система критериев оценивания, как и при проведении промежуточной аттестации по модулю, опирается на три уровня освоения компонентов компетенций: пороговый, повышенный, высокий.

Компоненты компетенций	**Признаки уровня освоения компонентов компетенций**		
	пороговый	**повышенный**	**высокий**
Знания	Студент демонстрирует знание-знакомство, знание-копию: узнает объекты, явления и понятия, находит в них различия, проявляет знание источников получения информации, может осуществлять самостоятельно репродуктивные действия над знаниями путем самостоятельного воспроизведения и применения информации.	Студент демонстрирует аналитические знания: уверенно воспроизводит и понимает полученные знания, относит их к той или иной классификационной группе, самостоятельно систематизирует их, устанавливает взаимосвязи между ними, продуктивно применяет в знакомых ситуациях.	Студент может самостоятельно извлекать новые знания из окружающего мира, творчески их использовать для принятия решений в новых и нестандартных ситуациях.
Умения	Студент умеет корректно выполнять предписанные действия по инструкции, алгоритму в известной ситуации, самостоятельно выполняет действия по решению типовых задач, требующих выбора из числа известных методов, в предсказуемо изменяющейся ситуации	Студент умеет самостоятельно выполнять действия (приемы, операции) по решению нестандартных задач, требующих выбора на основе комбинации известных методов, в непредсказуемо изменяющейся ситуации	Студент умеет самостоятельно выполнять действия, связанные с решением исследовательских задач, демонстрирует творческое использование умений (технологий)
Личностные качества	Студент имеет низкую мотивацию учебной деятельности, проявляет безразличное, безответственное отношение к учебе, порученному делу	Студент имеет выраженную мотивацию учебной деятельности, демонстрирует позитивное отношение к обучению и будущей трудовой деятельности, проявляет активность.	Студент имеет развитую мотивацию учебной и трудовой деятельности, проявляет настойчивость и увлеченность, трудолюбие, самостоятельность, творческий подход.

8.2. КРИТЕРИИ ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПРИ ИСПОЛЬЗОВАНИИ НЕЗАВИСИМОГО ТЕСТОВОГО КОНТРОЛЯ

При проведении независимого тестового контроля как формы промежуточной аттестации применяется методика оценивания результатов, предлагаемая разработчиками тестов. Процентные показатели результатов независимого тестового контроля переводятся в баллы промежуточной аттестации по 100-балльной шкале в БРС:

- в случае балльной оценки по тесту (блокам, частям теста) переводится процент набранных баллов от общего числа возможных баллов по тесту;
- при отсутствии балльной оценки по тесту переводится процент верно выполненных заданий теста, от общего числа заданий.

8.3. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

8.3.1. Примерные задания для проведения мини-контрольных в рамках учебных занятий

не предусмотрено

8.3.2. Примерные контрольные задачи в рамках учебных занятий

1. Определить время перебора всех паролей, состоящих из шести цифр. Алфавит составляют цифры n = 10. Длина пароля 6 символов k = 6. Принять скорость перебора s = 10 паролей в секунду. После каждого из m=3 неправильно введенных паролей идет пауза в v=5 секунд.
2. Определить минимальную длину пароля, алфавит которого состоит из 10 символов, время перебора которого было бы не меньше 10 лет. Алфавит составляют символы n = 10. Принять скорость перебора s = 10 паролей в секунду.
3. Определить время перебора всех паролей с параметрами. Алфавит состоит из n символов. Длина пароля символов k. Скорость перебора s паролей в секунду. После каждого из m неправильно введенных паролей идет пауза в v секунд.

Варианты заданий:

вариант	n	k	s	m	v
1	35	10	100	5	10
2	90	5	500	10	20
3	120	8	350	0	60
4	500	7	1000	3	15
5	60	12	200	5	30
6	320	4	450	10	10
7	110	6	650	7	60
8	65	5	1000	8	30
9	26	11	100	6	20
10	87	10	250	5	15

4. Определить минимальную длину пароля, алфавит которого состоит из n символов, время перебора которого было не меньше t лет. Скорость перебора s паролей в секунду.

Варианты заданий:

вариант	n	t	s
1	35	100	100
2	90	10	500
3	120	25	350
4	500	600	1000
5	60	1000	200
6	320	300	450
7	110	50	650
8	65	60	1000

9	26	400	100
10	87	300	250

5. Определить количество символов алфавита, пароль состоит из k символов, время перебора которого было не меньше t лет. Скорость перебора s паролей в секунду.
Варианты заданий:

вариант	k	t	s
1	5	100	100
2	6	10	500
3	10	25	350
4	7	600	1000
5	14	1000	200
6	20	300	450
7	4	50	650
8	8	60	1000
9	12	400	100
10	10	300	250

8.3.3. Примерные контрольные кейсы

не предусмотрено

8.3.4. Перечень примерных вопросов для зачета

- Основные понятия и определения из области информационной безопасности.
- Основные средства и методы аутентификации в компьютерных системах.
- Способы хранения паролей пользователей в виде хешей.
- Удаленная аутентификация.
- Протоколы CHAP и MS-CHAP.
- Трехсторонняя аутентификация в протоколе Kerberos.
- Семиуровневая модель OSI.
- Инкапсуляция и демультиплексирование.
- Протокол сетевого уровня IP.
- Протоколы транспортного уровня TCP и UDP.
- Протокол обработки ошибок ICMP.
- Виды и способы сетевых атак.
- Протокол SSH.
- Межсетевые и экраны. Классификация и характеристики.
- Трансляция сетевых адресов.
- Виды виртуальных частных сетей.
- Протокол IPSec. Создание VPN с использованием IPSec.
- Сканеры портов и уязвимостей.
- Системы обнаружения вторжения.

8.3.5. Перечень примерных вопросов для экзамена

не предусмотрено

8.3.6. Ресурсы АПИМ УрФУ, СКУД УрФУ для проведения тестового контроля в рамках текущей и промежуточной аттестации

не используются

8.3.7. Ресурсы ФЭПО для проведения независимого тестового контроля

не используются

8.3.8. Интернет-тренажеры

не используются

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«Уральский федеральный университет имени первого Президента России Б.Н. Ельцина»

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Криптографические методы защиты информации

Перечень сведений о рабочей программе дисциплины	**Учетные данные**
Модуль *Методы защиты информационных технических систем*	**Код модуля** 1140368
Образовательная программа *Информационные системы в научно-технических и социально-экономических технологиях*	**Код ОП 09.03.02/01.01** **Учебный план № 5456**
Направление подготовки *Информационные системы и технологии*	**Код направления и уровня подготовки** *09.03.02*
Уровень подготовки *Бакалавр*	
ФГОС ВО	**Реквизиты приказа Минобрнауки РФ об утверждении ФГОС ВО**: *Приказ от 12.03.2015, №219*

Екатеринбург, 2018

Рабочая программа дисциплины составлена авторами:

№ п/п	ФИО	Ученая степень, ученое звание	Должность	Кафедра	Подпись
1	Александров О.Е.	к.ф.-м.н., доцент	доцент	Технической физики	

Руководитель модуля К.В. Звонарев

Рекомендовано учебно-методическим советом института физико-технологического

Председатель учебно-методического совета В.В. Зверев
Протокол № _____ от _____ г.

Согласовано:

Дирекция образовательных программ Р.Х.Токарева

1. ОБЩАЯ ХАРАКТЕРИСТИКА ДИСЦИПЛИНЫ КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

1.1.Аннотация содержания дисциплины

Дисциплина «Криптографические методы защиты информации» относится к вариативной части образовательной программы (по выбору студента), входит в модуль «*Методы защиты информационных технических систем*». Изучение дисциплины позволит студентам овладеть знаниями в области основ теории и технологии криптографии – защиты информации от несанкционированного доступа, и освоить практическое применение этих технологий для задач профессиональной деятельности. Студенты обучаются практическому применению криптографической защиты информации на базе современных крипто алгоритмов, овладевают методами реализации прикладных задач криптографии на базе языков программирования и пакетов прикладных программ.

1.2. Язык реализации программы - русский

1.3. Планируемые результаты обучения по дисциплине

Результатом обучения в рамках дисциплины является формирование у студента следующих компетенций:

- способностью использовать основные законы естественнонаучных дисциплин в профессиональной деятельности, применять методы математического анализа и моделирования, теоретического и экспериментального исследования (ОПК-2);
- способностью использовать математические методы обработки, анализа и синтеза результатов профессиональных исследований (ПК-25);
- способностью поддерживать работоспособность информационных систем и технологий в заданных функциональных характеристиках и соответствии критериям качества (ПК-30);
- способностью обеспечивать безопасность и целостность данных информационных систем и технологий (ПК-31);

В результате освоения дисциплины студент должен:

Знать: задачи криптографии и подходы к построению криптографических систем; знать основные понятие криптографии; знать основные алгоритмы криптографического кодирования;

Уметь: применять методы криптографии для решения практических задач; реализовать прикладные задачи криптографии на базе языков программирования и пакетов прикладных программ;

Владеть: навыками применения криптографических алгоритмов.

1.4. Объем дисциплины

№ п/п	Виды учебной работы	Объем дисциплины		Распределение объема дисциплины по семестрам (час.)
		Всего часов	В т.ч. контактная работа (час.)*	8 семестр
1.	**Аудиторные занятия**	**64**	**64**	**64**
2.	Лекции	32	32	32
3.	Практические занятия	-	-	-
4.	Лабораторные работы	32	32	32
5.	**Самостоятельная работа студентов, включая все виды текущей аттестации**	134	9,6	134
6.	**Промежуточная аттестация**	18	2,33	**Экзамен, 18**
7.	**Общий объем по учебному плану, час.**	**216**	75,93	**216**
8.	**Общий объем по учебному плану, з.е.**	**6**		**6**

2. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Код раздела, темы	Раздел, тема дисциплины*	Содержание
Р1	Введение	Основные задачи криптографии и криптоанализа. Понятие криптопреобразования. Краткая справка по истории возникновения и развития, и современному криптографии.
Р2	Цифровое шифрование	Понятие несимметрии математических операций и трудоемкость элементарных математических операций. Понятие криптосистемы. Типы криптосистем. Криптосистемы с открытым ключом Понятие электронной подписи. Необходимость электронной подписи в криптосистемах с открытым ключом.
Р3	Конечные поля	Математическая теория групп как основа современных криптосистем. Основные математические понятия для конечного поля, характеристика поля. Возможность построения конечного поля с необходимым числом элементов. Мультипликативная группа конечного поля. Неприводимые многочлены. Порядок многочлена над конечным полем. Конструкция конечного поля из p^n элементов.
Р4	Последовательности над конечным полем	Псевдослучайные последовательности и их применение в криптографии.

		Алгебра последовательностей над конечным полем. Линейные рекуррентные последовательности над конечным полем. Аннулирующие многочлены. Регистр сдвига.
Р5	Дискретный логарифм	Экспоненциальный открытый ключ. Вычисление дискретного логарифма.
Р6	Линейные рекуррентные последовательности	Число появлений наборов фиксированной длины на полном периоде рекуррентной последовательности. Свойства решений линейного рекуррентного уравнения. Суммы с характерами. Максимальные линейные рекуррентные последовательности как псевдослучайные последовательности.

3. РАСПРЕДЕЛЕНИЕ УЧЕБНОГО ВРЕМЕНИ

3.1. Распределение аудиторной нагрузки и мероприятий самостоятельной работы по разделам дисциплины

Объем модуля (зач.ед.): 15
Объем дисциплины (зач.ед.):6

Раздел дисциплины			Аудиторные занятия (час.)				Самостоятельная работа: виды, количество и объемы мероприятий																						
Код раздела, темы	Наименование раздела, темы	**Всего по разделу, теме (час.)**	**Всего аудиторной работы (час.)**	Лекции	Практические занятия	Лабораторные работы	**Всего самостоятельной работы студентов (час.)**	Подготовка к аудиторным занятиям (час.)					Выполнение самостоятельных внеаудиторных работ (колич.)											Подготовка к контрольным мероприятиям текущей аттестации (колич.)			Подготовка к промежуточной аттестации по дисциплине (час.)		Подготовка в рамках дисциплины к промежуточной аттестации по модулю (час.)	
								Всего (час.)	Лекция	Практ., семинар. занятие	Лабораторное занятие	Н/и семинар, семинар-конфер., коллоквиум (магистратура)	**Всего (час.)**	Домашняя работа*	Графическая работа*	Реферат, эссе, творч. работа*	Проектная работа*	Расчетная работа, разработка программного продукта*	Расчетно-графическая работа*	Домашняя работа на иностр. языке*	Перевод иностр. литературы*	Курсовая работа*	Курсовой проект*	**Всего (час.)**	Контрольная работа*	Коллоквиум*	Зачет	Экзамен	Интегрированный экзамен по модулю	Проект по модулю
Р1	Введение	4	2	2			2	2	2																					
Р2	Цифровое шифрование	154	40	8		32	114	90	4		86		24									1								
Р3	Конечные поля	14	10	10			4	4	4																					
Р4	Последовательности над конечным полем	12	6	6			6	6	6																					
Р5	Дискретный логарифм	6	2	2			4	2	2																2	1				
Р6	Линейные рекуррентные последовательности	8	4	4			4	4	4																					
	Всего (час), без учета промежуточной аттестации:	**198**	**64**	**32**	**0**	**32**	**134**	**108**	**22**	**0**	**86**	**0**	**24**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**24**	**0**	**2**	**2**					
	Всего по дисциплине (час.):	**216**	**64**				**152**	В т.ч. промежуточная аттестация																			0	18	**0**	0

4. ОРГАНИЗАЦИЯ ПРАКТИЧЕСКИХ ЗАНЯТИЙ, САМОСТОЯТЕЛЬНОЙ РАБОТЫ ПО ДИСЦИПЛИНЕ

4.1. Лабораторные работы

Код раздела, темы	Номер работы	Наименование работы	Время на выполнение работы (час.)
P2	1	Криптографические алгоритмы. ГОСТ 28147-89	8
P2	2	Криптографические алгоритмы. Основы RSA	8
P2	3	Криптографические алгоритмы. Основы AES	8
P2	4	Криптоанализ. Взлом RSA	8
		Всего:	32

4.2. Практические занятия

не предусмотрено

4.3.Примерная тематика самостоятельной работы

4.3.1. Примерный перечень тем домашних работ
не предусмотрено

4.3.2. Примерный перечень тем графических работ
не предусмотрено

4.3.3. Примерный перечень тем рефератов (эссе, творческих работ)
не предусмотрено

4.3.4 Примерная тематика индивидуальных или групповых проектов
не предусмотрено

4.3.5. Примерный перечень тем расчетных работ (программных продуктов)
не предусмотрено

4.3.6. Примерный перечень тем расчетно-графических работ
не предусмотрено

4.3.7. Примерный перечень тем курсовых проектов (курсовых работ)

- Статистические свойства блочных алгоритмов шифрования.
- Криптографические свойства поточных шифров.
- Программная реализация алгоритма ГОСТ 28147-89.
- Программная реализация алгоритма RSA.
- Программная реализация алгоритма AES.
- Крипто анализ алгоритма RSA.
- Программная реализация алгоритма DES.
- Программная реализация алгоритма 3DES.
- Криптографические свойства хэш-функций.

4.3.8. Примерная тематика контрольных работ

- Конечные поля и их основные свойства.
- Неприводимые и примитивные многочлены над конечным полем.

4.3.9. Примерная тематика коллоквиумов
не предусмотрено

5. СООТНОШЕНИЕ РАЗДЕЛОВ, ТЕМ ДИСЦИПЛИНЫ И ПРИМЕНЯЕМЫХ ТЕХНОЛОГИЙ ОБУЧЕНИЯ

Код раздела, темы дисциплины	Активные методы обучения						Дистанционные образовательные технологии и электронное обучение					
	Проектная работа	Кейс-анализ	Деловые игры	Проблемное обучение	Командная работа	Другие (диалоговое обсуждение пройденного)	Сетевые учебные курсы	Виртуальные практикумы и тренажеры	Вебинары и видеоконференции	Асинхронные web-конференции и семинары	Совместная работа и разработка контента	Другие (указать, какие)
Р1-Р6				*	*							

6. ПРОЦЕДУРЫ КОНТРОЛЯ И ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ (Приложение 1)

7. ПРОЦЕДУРЫ ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ В РАМКАХ НЕЗАВИСИМОГО ТЕСТОВОГО КОНТРОЛЯ (Приложение 2)

8. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ (Приложение 3)

9. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

9.1.Рекомендуемая литература

9.1.1.Основная литература

1. Беломойцев Д. Е. , Волосатова Т. М. , Родионов С. В. Основные методы криптографической обработки данных: учебное пособие, Издательство МГТУ им. Н.Э. Баумана, 2014. - 80 с.; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book_view_red&book_id=258552
2. Лапонина, О.Р. Криптографические основы безопасности / О.Р. Лапонина. - М. : Национальный Открытый Университет «ИНТУИТ», 2016. - 244 с.; То же [Электронный ресурс]. - URL: //biblioclub.ru/index.php?page=book&id=429092.

9.1.2. Дополнительная литература

1. Кнауб Л.В. , Новиков Е.А. , Шитов Ю.А. Теоретико-численные методы в криптографии: учебное пособие, Сибирский федеральный университет, 2011. - 160 с.; То же [Электронный ресурс]. – URL: http://biblioclub.ru/index.php?page=book_view_red&book_id=229582
2. Фомичев В.М. Методы дискретной математики в криптологии, Диалог-МИФИ, 2010. - 436 с.; То же [Электронный ресурс]. – URL: http://biblioclub.ru/index.php?page=book_view_red&book_id=447668

3. Басалова Г.В. Основы криптографии: курс лекций, Интернет-Университет Информационных Технологий, 2011. - 253 с.; То же [Электронный ресурс]. – URL: http://biblioclub.ru/index.php?page=book_view_red&book_id=233689
4. Фороузан Б.А. Математика криптографии и теория шифрования, Национальный Открытый Университет «ИНТУИТ», 2016. - 511 с.; То же [Электронный ресурс]. – URL: http://biblioclub.ru/index.php?page=book_view_red&book_id=428998

9.2.Методические разработки

не используются.

9.3.Программное обеспечение

MathCAD, Microsoft Visual Studio.

9.4. Базы данных, информационно-справочные и поисковые системы

1. Государственная публичная научно-техническая библиотека: http://www/gpntb.ru
2. Библиотека УрФУ: http://lib.urfu.ru

9.5.Электронные образовательные ресурсы

http://212.193.94.130/КМЗИ/ или http://mp.fizteh.urfu.ru/КМЗИ/

10. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Сведения об оснащенности дисциплины специализированным и лабораторным оборудованием

Лекции и лабораторные работы проводятся в аудитории, оснащенной проектором с использованием мобильного компьютера (ноутбука). Компьютерный класс с установленным программным обеспечением п.9.3 и числом рабочих мест соответствующим числу студентов в группе. Допустимо один компьютер на двух обучающихся.

ПРИЛОЖЕНИЕ 1
к рабочей программе дисциплины

6. ПРОЦЕДУРЫ КОНТРОЛЯ И ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ В РАМКАХ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ

6.1. Весовой коэффициент значимости дисциплины – 1

6.2.Процедуры текущей и промежуточной аттестации по дисциплине

1.Лекции: **коэффициент значимости совокупных результатов лекционных занятий – 0,5**		
Текущая аттестация на лекциях	**Сроки – семестр, учебная неделя**	**Максимальная оценка в баллах**
Посещение лекций	8 семестр, 1 – 18 учебные недели	50
Контрольная работа	8 семестр, 17 – 18 учебные недели	50
Весовой коэффициент значимости результатов текущей аттестации по лекциям – 0,4		
Промежуточная аттестация по лекциям – экзамен **Весовой коэффициент значимости результатов промежуточной аттестации по лекциям – 0,6**		
2. Лабораторные занятия: коэффициент значимости совокупных результатов лабораторных занятий – 0,5		
Текущая аттестация на лабораторных занятиях	**Сроки – семестр, учебная неделя**	**Максимальная оценка в баллах**
Выполнение заданий	8 семестр, 10-18 учебная неделя	100
Весовой коэффициент значимости результатов текущей аттестации по лабораторным занятиям - 1		
Промежуточная аттестация по лабораторным занятиям– нет **Весовой коэффициент значимости результатов промежуточной аттестации по лабораторным занятиям– 0**		

6.3. Процедуры текущей и промежуточной аттестации курсовой работы

Текущая аттестация выполнения курсовой работы	**Сроки − семестр, учебная неделя**	**Максимальная оценка в баллах**
Выполнение заданий	8 семестр, 10-18 учебная неделя	100
Весовой коэффициент текущей аттестации выполнения курсовой работы – 0.5		
Весовой коэффициент промежуточной аттестации выполнения курсовой работы – защиты – 0.5		

6.4. Коэффициент значимости семестровых результатов освоения дисциплины

Не предусмотрено

ПРИЛОЖЕНИЕ 2
к рабочей программе дисциплины

7. ПРОЦЕДУРЫ ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ В РАМКАХ НЕЗАВИСИМОГО ТЕСТОВОГО КОНТРОЛЯ

Дисциплина и ее аналоги, по которым возможно тестирование, отсутствуют на сайте ФЭПО http://fepo.i-exam.ru.

Дисциплина и ее аналоги, по которым возможно тестирование, отсутствуют на сайте Интернет-тренажеры http://training.i-exam.ru.

Дисциплина и ее аналоги, по которым возможно тестирование, отсутствуют на портале СМУДС УрФУ.

В связи с отсутствием Дисциплины и ее аналогов, по которым возможно тестирование, на сайтах ФЭПО, Интернет-тренажеры и портале СМУДС УрФУ, тестирование в рамках НТК не проводится.

ПРИЛОЖЕНИЕ 3
к рабочей программе дисциплины

8. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ

8.1. КРИТЕРИИ ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ КОНТРОЛЬНО-ОЦЕНОЧНЫХ МЕРОПРИЯТИЙ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ В РАМКАХ БРС

В рамках БРС применяются утвержденные на кафедре критерии оценивания достижений студентов по каждому контрольно-оценочному мероприятию. Система критериев оценивания, как и при проведении промежуточной аттестации по модулю, опирается на три уровня освоения компонентов компетенций: пороговый, повышенный, высокий.

Компоненты компетенций	**Признаки уровня освоения компонентов компетенций**		
	пороговый	**повышенный**	**высокий**
Знания	Студент демонстрирует знание-знакомство, знание-копию: узнает объекты, явления и понятия, находит в них различия, проявляет знание источников получения информации, может осуществлять самостоятельно репродуктивные действия над знаниями путем самостоятельного воспроизведения и применения информации.	Студент демонстрирует аналитические знания: уверенно воспроизводит и понимает полученные знания, относит их к той или иной классификационной группе, самостоятельно систематизирует их, устанавливает взаимосвязи между ними, продуктивно применяет в знакомых ситуациях.	Студент может самостоятельно извлекать новые знания из окружающего мира, творчески их использовать для принятия решений в новых и нестандартных ситуациях.
Умения	Студент умеет корректно выполнять предписанные действия по инструкции, алгоритму в известной ситуации, самостоятельно выполняет действия по решению типовых задач, требующих выбора из числа известных методов, в предсказуемо изменяющейся ситуации	Студент умеет самостоятельно выполнять действия (приемы, операции) по решению нестандартных задач, требующих выбора на основе комбинации известных методов, в непредсказуемо изменяющейся ситуации	Студент умеет самостоятельно выполнять действия, связанные с решением исследовательских задач, демонстрирует творческое использование умений (технологий)
Личностные качества	Студент имеет низкую мотивацию учебной деятельности, проявляет безразличное, безответственное отношение к учебе, порученному делу	Студент имеет выраженную мотивацию учебной деятельности, демонстрирует позитивное отношение к обучению и будущей трудовой деятельности, проявляет активность.	Студент имеет развитую мотивацию учебной и трудовой деятельности, проявляет настойчивость и увлеченность, трудолюбие, самостоятельность, творческий подход.

8.2. КРИТЕРИИ ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПРИ ИСПОЛЬЗОВАНИИ НЕЗАВИСИМОГО ТЕСТОВОГО КОНТРОЛЯ

При проведении независимого тестового контроля как формы промежуточной аттестации применяется методика оценивания результатов, предлагаемая разработчиками тестов. Процентные показатели результатов независимого тестового контроля переводятся в баллы промежуточной аттестации по 100-балльной шкале в БРС:

- в случае балльной оценки по тесту (блокам, частям теста) переводится процент набранных баллов от общего числа возможных баллов по тесту;
- при отсутствии балльной оценки по тесту переводится процент верно выполненных заданий теста, от общего числа заданий.

8.3. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

8.3.1. Примерные задания для проведения мини-контрольных в рамках учебных занятий

не предусмотрено

8.3.2. Примерные контрольные задачи в рамках учебных занятий

Примерный вариант контрольной работы №1

Вариант 1

1. Применяя алгоритм Евклида, найти НОД(a, b) и НОК(a, b) для следующих чисел:
$$a = 126,\ b = 525.$$
2. Решить следующую систему сравнений
$$\begin{cases} 2x + 3y \equiv 1 (\mathrm{mod}\ 26), \\ 7x + 8y \equiv 2 (\mathrm{mod}\ 26). \end{cases}$$
3. Методом Кронекера найти каноническое разложение многочлена
$$f(x) = \frac{1}{3}x^6 - \frac{5}{3}x^5 + 2x^4 - x^3 + 5x^2 - \frac{17}{3}x - 1 \in \mathrm{Q}[x].$$
4. Построить таблицы сложения и умножения для факторкольца $\mathrm{F}_2[x]/(x^3 + x^2 + x)$. Определить, будет ли это кольцо полем.

Вариант 2

1. Применяя алгоритм Евклида, найти НОД(a, b) и НОК(a, b) для следующих чисел:
$$a = 1541\ ,\ b = 1817.$$
2. Решить следующую систему сравнений
$$\begin{cases} 5x \equiv 20 (\mathrm{mod}\ 6), \\ 6x \equiv 6 (\mathrm{mod}\ 5), \\ 4x \equiv 5 (\mathrm{mod}\ 77). \end{cases}$$
3. Методом Кронекера найти каноническое разложение многочлена
$$f = \frac{1}{3}x^6 + 4x^5 + 19x^4 + 45\frac{1}{3}x^3 + 57x^2 + 36x + 9 \in \mathrm{Q}[x].$$
4. Построить таблицы сложения и умножения для факторкольца $\mathrm{F}_2[x]/(x^3 + x)$. Определить, будет ли это кольцо полем.

Примерный вариант контрольной работы № 2

Вариант 1

1. Применяя алгоритм Евклида, найти НОД(f, g) для следующих многочленов над полем F:

$$F = F_2, f(x) = x^7 + 1, g(x) = x^5 + x^3 + x + 1.$$

2. Используя производную многочлена выяснить, имеет ли следующий многочлен кратные корни:

$$f(x) = x^6 + x^5 + x^4 + x^3 + 1 \in F_2[x].$$

3. Вычислить дискриминант $D(f)$ многочлена f и с его помощью выяснить, имеет или нет многочлен кратные корни:

$$f(x) = 2x^4 + x^3 + x^2 + 2x + 2 \in F_3[x].$$

4. Вычислить результант $R(f, g)$ двух многочленов f и g и выяснить, имеют или нет эти многочлены общие корни:

$$f(x) = x^4 + x^3 + 1, \quad g(x) = x^4 + x^2 + x + 1 \in F_2[x].$$

5. Найти все примитивные элементы поля F_7.
6. Найти первообразные корни 4-й и 8-й степени из единицы в поле F_9.
7. Найти порядок многочлена $x^7 - x^6 + x^4 - x^2 + x$ над полем F_3.
8. Найти все примитивные многочлены степени 2 над полем F_3.

Вариант 2.

1. Применяя алгоритм Евклида, найти НОД(f, g) для следующих многочленов над полем F:

$$F = F_2, f(x) = x^5 + x + 1, g(x) = x^6 + x^5 + x^4 + 1.$$

2. Используя производную многочлена выяснить, имеет ли следующий многочлен кратные корни:

$$f(x) = x^4 - 5x^3 + 6x^2 + 4x - 8 \in Q[x].$$

3. Вычислить дискриминант $D(f)$ многочлена f и с его помощью выяснить, имеет или нет многочлен кратные корни:

$$f(x) = 2x^3 - 3x^2 + x + 1 \in Q[x].$$

4. Вычислить результант $R(f, g)$ двух многочленов f и g и выяснить, имеют или нет эти многочлены общие корни:

$$f(x) = x^3 + x + 1, \quad g(x) = 2x^5 + x^2 + 2 \in F_3[x].$$

5. Найти все примитивные элементы поля F_{17}.
6. Найти первообразные корни 9-й степени из единицы в поле F_{19}.
7. Найти порядок многочлена $(x^2 + x + 1)^5(x^3 + x + 1)$ над полем F_2.
8. Найти все примитивные многочлены степени 2 над полем F_4.

8.3.3. Примерные контрольные кейсы

не предусмотрено

8.3.4. Перечень примерных вопросов для зачета

не предусмотрено

8.3.5. Перечень примерных вопросов для экзамена

1) История криптографии. Обзор криптосистем прошлого.
2) Трудоемкость арифметических операций.
3) Возведение в степень.
4) Отыскание наибольшего общего делителя.
5) Решение диофантова уравнения первой степени.
6) Решение сравнения первой степени.
7) Разложение на множители натуральных чисел и распознавание простоты.
8) Криптосистемы без передачи ключей.
9) Криптосистема с открытым ключом.
10) Электронная подпись.
11) Конечные поля. Определение.
12) Характеристика поля.
13) Существование конечного поля.
14) Мультипликативная группа конечного поля.
15) Неприводимые над конечным полем многочлены.
16) Порядок многочлена над конечным полем.

17) Примитивные над конечным полем многочлены.
18) Конструкция конечного поля из p^n элементов.
19) Последовательности над конечным полем.
20) Псевдослучайные последовательности и их применение в криптографии.
21) Алгебра последовательностей.
22) Линейные рекуррентные последовательности над конечным полем.
23) Аннулирующие многочлены.
24) Регистр сдвига.
25) Дискретный логарифм.
26) Экспоненциальный открытый ключ.
27) Вычисление дискретного логарифма.
28) Линейные рекуррентные последовательности как псевдослучайные последовательности.
29) Число появлений наборов фиксированных знаков на полном периоде лин. рекуррентной последовательности.
30) Свойства решений лин. рекуррентного уравнения.

8.3.6. Ресурсы АПИМ УрФУ, СКУД УрФУ для проведения тестового контроля в рамках текущей и промежуточной аттестации

не используются

8.3.7. Ресурсы ФЭПО для проведения независимого тестового контроля

не используются

8.3.8. Интернет-тренажеры

не используются

8.3.9. Примерные задания для курсовых работ

Курсовая работа должна иметь следующую структуру: титульный лист, содержание, введение, 3-4 тематических главы, заключение, список использованных источников. При необходимости добавления объёмного иллюстративного материала (листинг программ, блок-схемы, объёмные расчеты и т.п.) допускается одно или несколько приложений в конце курсовой работы. Объём работы должен составлять 15-45 страниц А4 при использовании шрифта Times New Roman 14 и полуторного междустрочного интервала. Защита курсовой работы происходит в установленные преподавателем сроки в виде доклада с презентацией на 5-10 слайдов.

Примерный список заданий к курсовым работам:

1. Разработать алгоритм и программу (с использованием любого языка программирования) по исследованию статистических свойств блочных алгоритмов шифрования.
2. Разработать алгоритм и программу (с использованием любого языка программирования) разложения целых чисел для анализа шифра RSA.
3. Разработать алгоритм и программу (с использованием любого языка программирования) по анализу шифра AES.
4. Разработать алгоритм и программу (с использованием любого языка программирования) реализации и исследования хэш-функций.
5. Разработать алгоритм и программу (с использованием любого языка программирования) по анализу криптосистем с открытым ключами на основе сложности дискретного логарифмирования.
6. Разработать лабораторную работу по анализу криптосистем с открытыми ключами на основе свойств эллиптических кривых.
7. Разработать алгоритм и программу (с использованием любого языка программирования) по линейному анализу криптографических примитивов и блочных шифров.
8. Разработать программный комплекс по анализу поточного шифрования алгоритмом RC4.
9. Разработать лабораторную работу по дифференциальному анализу криптографических примитивов блочных шифров.

10. Разработать программу (с использованием любого языка программирования) реализующую блочный шифр ГОСТ 28147-89 в различных режимах.
11. Разработать лабораторную работу по криптографическому анализу шифра DES.
12. Разработать лабораторную работу по криптографическому анализу шифра 3DES.
13. Разработать алгоритм и программу (с использованием любого языка программирования) блочного шифрования 128-битовых данных на основе линейных и нелинейных преобразований.
14. Разработать лабораторную работу по анализу RSA подобных криптографических систем.
15. Разработать и реализовать программный комплекс для исследования свойств криптографических ключей.

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«Уральский федеральный университет имени первого Президента России Б.Н. Ельцина»

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Основы теории алгоритмов и анализа их сложности

Перечень сведений о рабочей программе дисциплины	**Учетные данные**
Модуль *Методы защиты информационных технических систем*	**Код модуля** 1140368
Образовательная программа *Информационные системы в научно-технических и социально-экономических технологиях*	**Код ОП 09.03.02/01.01** **Учебный план № 5456**
Направление подготовки *Информационные системы и технологии*	**Код направления и уровня подготовки** *09.03.02*
Уровень подготовки *Бакалавр*	
ФГОС ВО	**Реквизиты приказа Минобрнауки РФ об утверждении ФГОС ВО**: *Приказ от 12.03.2015, №219*

Екатеринбург, 2018

Рабочая программа дисциплины составлена авторами:

№ п/п	ФИО	Ученая степень, ученое звание	Должность	Кафедра	Подпись
1	Иванов А.Г.	к.ф.-м.н.	доцент	Технической физики	

Руководитель модуля К.В. Звонарев

Рекомендовано учебно-методическим советом института физико-технологического

Председатель учебно-методического совета В.В. Зверев
Протокол № _____ от _____ г.

Согласовано:

Дирекция образовательных программ Р.Х.Токарева

1. ОБЩАЯ ХАРАКТЕРИСТИКА ДИСЦИПЛИНЫ ОСНОВЫ ТЕОРИИ АЛГОРИТМОВ И АНАЛИЗА ИХ СЛОЖНОСТИ

1.1.Аннотация содержания дисциплины

Дисциплина «Основы теории алгоритмов и анализа их сложности» относится к вариативной части образовательной программы (по выбору студента), входит в модуль «*Методы защиты информационных технических систем*». В процессе освоения дисциплины студентам предоставляется возможность получить комплексное всестороннее представление об основах математической логики, теории алгоритмов, методах оценки сложности алгоритмов и построения эффективных алгоритмов. Полученные в рамках дисциплины «*Основы теории алгоритмов и анализа их сложности*» знания могут использоваться при проектировании новых и анализе существующих подсистем защиты в информационно-технических системах.

1.2. Язык реализации программы - русский

1.3. Планируемые результаты обучения по дисциплине

Результатом обучения в рамках дисциплины является формирование у студента следующих компетенций:

способностью использовать основные законы естественнонаучных дисциплин в профессиональной деятельности, применять методы математического анализа и моделирования, теоретического и экспериментального исследования (ОПК-2);
- способностью использовать технологии разработки объектов профессиональной деятельности в областях: безопасность информационных систем, управление технологическими процессами, техническая физика, энергетика, ядерная энергетика, в условиях экономики информационного общества (ПК-17);
способностью использовать математические методы обработки, анализа и синтеза результатов профессиональных исследований (ПК-25);
- способностью обеспечивать безопасность и целостность данных информационных систем и технологий (ПК-31);

В результате освоения дисциплины студент должен:

Знать: возможности применения логических и алгоритмических методов в криптографии; подходы к оценкам сложности алгоритмов и методы построения эффективных алгоритмов; представления булевых функций и способы минимизации формул;

Уметь: оценивать сложность алгоритмов и вычислений; классифицировать алгоритмы по классам сложности;

Владеть: навыками применения средств математической логики; навыками применения методов и фактов теории алгоритмов, относящимися к решению переборных задач.

1.4. Объем дисциплины

№ п/п	Виды учебной работы	Объем дисциплины		Распределение объема дисциплины по семестрам (час.)
		Всего часов	В т.ч. контактная работа (час.)*	7 семестр
1.	**Аудиторные занятия**	**51**	**51**	**51**
2.	Лекции	34	34	34
3.	Практические занятия	-	-	-
4.	Лабораторные работы	17	17	17
5.	**Самостоятельная работа студентов, включая все виды текущей аттестации**	39	7,65	39
6.	**Промежуточная аттестация**	18	2,33	**Экзамен, 18**
7.	**Общий объем по учебному плану, час.**	**108**	60,98	**108**
8.	**Общий объем по учебному плану, з.е.**	**3**		**3**

2. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Код раздела, темы	Раздел, тема дисциплины*	Содержание
Р1	Введение	Предмет математической логики. Теория доказательств и теория моделей. Основные исторические сведения: силлогистика Аристотеля. Основания математики и парадоксы теории множеств. Программа спасения классической математики. Аксиоматический метод. Теорема неполноты. Исследование математических теорий, непротиворечивость, полнота, разрешимость. Применение символьных языков для записи математических утверждений.
Р2	Алгебра логики	Понятие алгебраической системы. Булевы алгебры. Алгебра высказываний. Логические операции. Алгебра предикатов. Истинностное значение формулы. Интерпретация и модель. Отношение следования и равносильности. Булевы функции и нормальные формы. Теорема Поста.
Р3	Логические исчисления	Исчисление высказываний. Общее понятие о логическом исчислении. Аксиомы и правила вывода. Доказуемость и выводимость формул. Теорема дедукции. Непротиворечивость и полнота исчисления высказываний. Исчисление предикатов. Аксиомы и правила вывода в исчислении предикатов. Вспомогательные правила выводаю Семантика исчисления предикатов. Интерпретация языка исчисления. Непротиворечивость и полнота исчисления предикатов. Теорема

		Мальцева.
Р4	Алгоритмические модели	Понятие алгоритма. Необходимость уточнения интуитивного определения алгоритма. Основные алгоритмические модели. Машины Тьюринга. Вычислимость по Тьюрингу. Тезис Тьюринга. Частично-рекурсивные функции (ЧРФ). Тезис Чёрча. Соотношение между классами «Т» и «Ч». Вычислимость по Тьюрингу ЧРФ. Нумерации наборов чисел и слов. Частичная рекурсивность Т-вычислимых функций. Нумерация алгоритмов. Невычислимые функции. Алгоритмически неразрешимые проблемы.
Р5	Сложность вычислений	Характеристики сложности. Временная и емкостная сложность машины Тьюринга. Основные теоремы о сложности. Прямые нижние оценки временной сложности вычислений. Классы сложности «Р» и «NP». NP-полные задачи. Теорема Кука. Примеры NP-полных задач. Сильная NP-полнота.

3. РАСПРЕДЕЛЕНИЕ УЧЕБНОГО ВРЕМЕНИ

3.1. Распределение аудиторной нагрузки и мероприятий самостоятельной работы по разделам дисциплины

Объем модуля (зач.ед.): 15
Объем дисциплины (зач.ед.): 3

Раздел дисциплины			Аудиторные занятия (час.)				Самостоятельная работа: виды, количество и объемы мероприятий																					
Код раздела, темы	Наименование раздела, темы	**Всего по разделу, теме (час.)**	**Всего аудиторной работы (час.)**	Лекции	Практические занятия	Лабораторные работы	**Всего самостоятельной работы студентов (час.)**	Подготовка к аудиторным занятиям (час.)					Выполнение самостоятельных внеаудиторных работ (колич.)											Подготовка к контрольным мероприятиям текущей аттестации (колич.)			Подготовка к промежуточной аттестации по дисциплине (час.)		Подготовка в рамках дисциплины к промежуточной аттестации по модулю (час.)	
								Всего (час.)	Лекция	Практ., семинар. занятие	Лабораторное занятие	Н/и семинар, семинар-конфер., коллоквиум (магистратура)	**Всего (час.)**	Домашняя работа*	Графическая работа*	Реферат, эссе, творч. работа*	Проектная работа*	Расчетная работа, разработка программного продукта*	Расчетно-графическая работа*	Домашняя работа на иностр. языке*	Перевод иностр. литературы*	Курсовая работа*	Курсовой проект*	**Всего (час.)**	Контрольная работа*	Коллоквиум*	Зачет	Экзамен	Интегрированный экзамен по модулю	Проект по модулю
Р1	Введение	4	2	2			2	2	2																			
Р2	Алгебра логики	19	11	8		3	8	8	4		4																	
Р3	Логические исчисления	20	12	8		4	8	8	4		4																	
Р4	Алгоритмические модели	23	14	8		6	9	9	4		4																	
Р5	Сложность вычислений	24	12	8		4	12	12	6		7																	
	Всего (час), без учета промежуточной аттестации:	**90**	**51**	**34**	**0**	**17**	**39**	**39**	**20**	**0**	**19**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**			
	Всего по дисциплине (час.):	**108**	**51**				**57**	В т.ч. промежуточная аттестация																			0	18	**0**	0

4. ОРГАНИЗАЦИЯ ПРАКТИЧЕСКИХ ЗАНЯТИЙ, САМОСТОЯТЕЛЬНОЙ РАБОТЫ ПО ДИСЦИПЛИНЕ

4.1. Лабораторные работы

Код раздела, темы	Номер занятия	Тема занятия	Время на проведение занятия (час.)
Р2	1	Алгебра логики. Истинностное значение формулы алгебры предикатов	3
Р3	2	Вывод и доказательство в логическом исчислении	2
Р3	3	Вспомогательные правила вывода.	2
Р4	4	Машины Тьюринга	2
Р4	5	ЧРФ	2
Р4	6	Алгоритмически неразрешимые проблемы	2
Р5	7	Оценка сложности вычислений переборных задач	2
Р5	8	Сложность рекурсивных алгоритмов	2
		Всего:	17

4.2. Практические занятия

не предусмотрено

4.3.Примерная тематика самостоятельной работы

4.3.1. Примерный перечень тем домашних работ
не предусмотрено

4.3.2. Примерный перечень тем графических работ
не предусмотрено

4.3.3. Примерный перечень тем рефератов (эссе, творческих работ)
не предусмотрено

4.3.4 Примерная тематика индивидуальных или групповых проектов
не предусмотрено

4.3.5. Примерный перечень тем расчетных работ (программных продуктов)
не предусмотрено

4.3.6. Примерный перечень тем расчетно-графических работ
не предусмотрено

4.3.7. Примерный перечень тем курсовых проектов (курсовых работ)
не предусмотрено

4.3.8. Примерная тематика контрольных работ
не предусмотрено

4.3.9. Примерная тематика коллоквиумов
не предусмотрено

5. СООТНОШЕНИЕ РАЗДЕЛОВ, ТЕМ ДИСЦИПЛИНЫ И ПРИМЕНЯЕМЫХ ТЕХНОЛОГИЙ ОБУЧЕНИЯ

Код раздела, темы дисциплины	Активные методы обучения	Дистанционные образовательные технологии и электронное обучение

	Проектная работа	Кейс-анализ	Деловые игры	Проблемное обучение	Командная работа	Другие (диалоговое обсуждение пройденного)	Сетевые учебные курсы	Виртуальные практикумы и тренажеры	Вебинары и видеоконференции	Асинхронные web-конференции и семинары	Совместная работа и разработка контента	Другие (указать, какие)
Р1-Р5				*	*							

6. ПРОЦЕДУРЫ КОНТРОЛЯ И ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ (Приложение 1)

7. ПРОЦЕДУРЫ ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ В РАМКАХ НЕЗАВИСИМОГО ТЕСТОВОГО КОНТРОЛЯ (Приложение 2)

8. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ (Приложение 3)

9. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

9.1.Рекомендуемая литература

9.1.1.Основная литература

1. Ершов, Ю.Л. Математическая логика. [Электронный ресурс] / Ю.Л. Ершов, Е.А. Палютин. — Электрон. дан. — М. : Физматлит, 2011. — 356 с. — Режим доступа: http://e.lanbook.com/book/59599.
2. Глухов, М.М. Математическая логика. Дискретные функции. Теория алгоритмов. [Электронный ресурс] / М.М. Глухов, А.Б. Шишков. — Электрон. дан. — СПб. : Лань, 2012. — 416 с. — Режим доступа: http://e.lanbook.com/book/4041.

9.1.2. Дополнительная литература

1. Математическая логика. Введение в математическую логику : [учебное пособие для студентов математических специальностей вузов] / А. Н. Колмогоров, А. Г. Драгалин ; Московский гос. ун-т им. М. В. Ломоносова .— Изд. 5-е .— Москва : ЛЕНАНД, 2015 .— 233, [1] с. — (Классический университетский учебник) 15 экз
2. Лавров, И.А. Задачи по теории множеств, математической логике и теории алгоритмов [Электронный ресурс] : учеб. / И.А. Лавров, Л.Л. Максимова. — Электрон. дан. — Москва : Физматлит, 2002. — 256 с. — Режим доступа: https://e.lanbook.com/book/2242.
3. Клини С.К. Математическая логика, Мир, 1973. - 479 с.; URL: http://biblioclub.ru/index.php?page=book&id=458243
4. Важенин Ю. М. Множества, логика, алгоритмы, Екатеринбург, УрГУ, 1995.
5. Зюзьков В.М. Математическая логика и теория алгоритмов: учебное пособие, Эль Контент, 2015. - 236 с.; То же [Электронный ресурс]. – URL: http://biblioclub.ru/index.php?page=book_view_red&book_id=480935

9.2.Методические разработки

не используются.

9.3.Программное обеспечение

не используется

9.4. Базы данных, информационно-справочные и поисковые системы

1. Государственная публичная научно-техническая библиотека: http://www/gpntb.ru
2. Библиотека УрФУ: http://lib.urfu.ru

9.5.Электронные образовательные ресурсы

не используются.

10. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Сведения об оснащенности дисциплины специализированным и лабораторным оборудованием

Лекции и лабораторные работы проводятся в аудитории, оснащенной проектором с использованием мобильного компьютера (ноутбука). Компьютерный класс с установленным программным обеспечением п.9.3 и числом рабочих мест соответствующим числу студентов в группе. Допустимо один компьютер на двух обучающихся.

ПРИЛОЖЕНИЕ 1
к рабочей программе дисциплины

6. ПРОЦЕДУРЫ КОНТРОЛЯ И ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ В РАМКАХ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ

6.1. Весовой коэффициент значимости дисциплины – 1

6.2.Процедуры текущей и промежуточной аттестации по дисциплине

1.Лекции: коэффициент значимости совокупных результатов лекционных занятий – 0,7		
Текущая аттестация на лекциях	**Сроки – семестр, учебная неделя**	**Максимальная оценка в баллах**
Посещение лекций	7 семестр, 1 – 18 учебные недели	100
Весовой коэффициент значимости результатов текущей аттестации по лекциям – 0,4		
Промежуточная аттестация по лекциям – экзамен **Весовой коэффициент значимости результатов промежуточной аттестации по лекциям – 0,6**		
2. Лабораторные занятия: коэффициент значимости совокупных результатов лабораторных занятий – 0,3		
Текущая аттестация на лабораторных занятиях	**Сроки – семестр, учебная неделя**	**Максимальная оценка в баллах**
Посещение занятий	7 семестр,	50

	9-18 учебная неделя	
Решение задач	7 семестр, 9-18 учебная неделя	50
Весовой коэффициент значимости результатов текущей аттестации по лабораторным занятиям - 1		
Промежуточная аттестация по лабораторным занятиям – нет **Весовой коэффициент значимости результатов промежуточной аттестации по лабораторным занятиям– 0**		

6.3. Процедуры текущей и промежуточной аттестации курсовой работы/проекта
Не предусмотрено

6.4. Коэффициент значимости семестровых результатов освоения дисциплины
Не предусмотрено

ПРИЛОЖЕНИЕ 2
к рабочей программе дисциплины

7. ПРОЦЕДУРЫ ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ В РАМКАХ НЕЗАВИСИМОГО ТЕСТОВОГО КОНТРОЛЯ

Дисциплина и ее аналоги, по которым возможно тестирование, отсутствуют на сайте ФЭПО http://fepo.i-exam.ru.

Дисциплина и ее аналоги, по которым возможно тестирование, отсутствуют на сайте Интернет-тренажеры http://training.i-exam.ru.

Дисциплина и ее аналоги, по которым возможно тестирование, отсутствуют на портале СМУДС УрФУ.

В связи с отсутствием Дисциплины и ее аналогов, по которым возможно тестирование, на сайтах ФЭПО, Интернет-тренажеры и портале СМУДС УрФУ, тестирование в рамках НТК не проводится.

ПРИЛОЖЕНИЕ 3
к рабочей программе дисциплины

8. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ

8.1. КРИТЕРИИ ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ КОНТРОЛЬНО-ОЦЕНОЧНЫХ МЕРОПРИЯТИЙ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ В РАМКАХ БРС

В рамках БРС применяются утвержденные на кафедре критерии оценивания достижений студентов по каждому контрольно-оценочному мероприятию. Система критериев оценивания, как и при проведении промежуточной аттестации по модулю, опирается на три уровня освоения компонентов компетенций: пороговый, повышенный, высокий.

Компоненты компетенций	**Признаки уровня освоения компонентов компетенций**		
	пороговый	**повышенный**	**высокий**
Знания	Студент демонстрирует знание-знакомство, знание-копию: узнает объекты, явления и понятия, находит в них различия, проявляет знание источников получения информации, может осуществлять самостоятельно репродуктивные действия над знаниями путем самостоятельного воспроизведения и применения информации.	Студент демонстрирует аналитические знания: уверенно воспроизводит и понимает полученные знания, относит их к той или иной классификационной группе, самостоятельно систематизирует их, устанавливает взаимосвязи между ними, продуктивно применяет в знакомых ситуациях.	Студент может самостоятельно извлекать новые знания из окружающего мира, творчески их использовать для принятия решений в новых и нестандартных ситуациях.
Умения	Студент умеет корректно выполнять предписанные действия по инструкции, алгоритму в известной ситуации, самостоятельно выполняет действия по решению типовых задач, требующих выбора из числа известных методов, в предсказуемо изменяющейся ситуации	Студент умеет самостоятельно выполнять действия (приемы, операции) по решению нестандартных задач, требующих выбора на основе комбинации известных методов, в непредсказуемо изменяющейся ситуации	Студент умеет самостоятельно выполнять действия, связанные с решением исследовательских задач, демонстрирует творческое использование умений (технологий)
Личностные качества	Студент имеет низкую мотивацию учебной деятельности, проявляет безразличное, безответственное отношение к учебе, порученному делу	Студент имеет выраженную мотивацию учебной деятельности, демонстрирует позитивное отношение к обучению и будущей трудовой деятельности, проявляет активность.	Студент имеет развитую мотивацию учебной и трудовой деятельности, проявляет настойчивость и увлеченность, трудолюбие, самостоятельность, творческий подход.

8.2. КРИТЕРИИ ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПРИ ИСПОЛЬЗОВАНИИ НЕЗАВИСИМОГО ТЕСТОВОГО КОНТРОЛЯ

При проведении независимого тестового контроля как формы промежуточной аттестации применяется методика оценивания результатов, предлагаемая разработчиками тестов. Процентные показатели результатов независимого тестового контроля переводятся в баллы промежуточной аттестации по 100-балльной шкале в БРС:

- в случае балльной оценки по тесту (блокам, частям теста) переводится процент набранных баллов от общего числа возможных баллов по тесту;
- при отсутствии балльной оценки по тесту переводится процент верно выполненных заданий теста, от общего числа заданий.

8.3. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

8.3.1. Примерные задания для проведения мини-контрольных в рамках учебных занятий
не предусмотрено

8.3.2. Примерные контрольные задачи в рамках учебных занятий
не предусмотрено

8.3.3. Примерные контрольные кейсы
не предусмотрено

8.3.4. Перечень примерных вопросов для зачета
не предусмотрено

8.3.5. Перечень примерных вопросов для экзамена

- Понятие алгебраической системы; алгебры и модели, примеры алгебраических систем. Булевы алгебры, алгебра высказываний и алгебра предикатов.
- Алгебра высказываний, определение высказывания, пропозициональные связки, логические операции и их свойства, выражение одних операций через другие.
- Алгебра предикатов, понятие предиката на множестве, логические операции с предикатами и их свойства, свободные и связанные переменные, определение формулы алгебры предикатов.
- Истинностное значение формулы, интерпретация и модель, таблицы истинности, общезначимые, выполнимые формулы и противоречия.
- Отношение следования и равносильность. Теорема о следовании. Основные соотношения равносильности. Использование равносильности для преобразования формул.
- Булевы функции: способы задания, унарные и бинарные операции, приоритеты, свойства операций. Полные системы функций, теорема Поста.
- Нормальные формы, алгоритмы построения ДНФ и КНФ. Полиномы Жегалкина
- Понятие вывода. Правила вывода и аксиомы исчисления высказываний. Доказуемость и выводимость. Отличие от общезначимости
- Непротиворечивость и полнота исчисления высказываний. Эквивалентность логики и исчисления высказываний

- Вывод в исчислении предикатов. Схемы аксиом и правила вывода. Выводимость и доказуемость. Особенности вывода в исчислении предикатов. Фиксированные переменные. Преимущество дедуктивного подхода по сравнению с семантическим.

- Исчисление предикатов: теорема о дедукции, вспомогательные правила вывода, применение вспомогательных правил, правила для эквивалентных (равносильных формул)

- Понятие доказуемой секвенции. Применение секвенций для упрощения выводов. Вспомогательные правила вывода. Теорема об импликации и доказуемости. Теорема о дедукции

- Определение выполнимой и общезначимой формулы. Непротиворечивость исчисления предикатов

- Полнота исчисления предикатов: выполнимое, непротиворечивое и полное множества формул; теорема о существовании непротиворечивого и полного множества формул; теорема о выполнимости; теорема о полноте

- Прямая и обратная теоремы о выполнимости. Теорема о совместной выполнимости. Теорема об адекватности. Теорема о компактности Мальцева.

- Понятие алгоритма. Алгоритмические модели

- Устройство и работа одноленточной машины Тьюринга. Функции, вычислимые по Тьюрингу. Примеры. Свойства машин. Тьюринга Тезис Тьюринга.

- Частично-рекурсивные функции. Примеры ЧРФ. Тезис Чёрча

- Соотношение между классами «Т» и «Ч». Т-вычислимость ЧРФ.

- Канторовская нумерация наборов чисел и слов.

- Нумерация машин Тьюринга. Перечисление ЧРФ. Невычислимые функции

- Нумерация машин Тьюринга. Универсальная функция. Существование универсальной ЧРФ одноместных и к-местных ЧРФ

- Массовые алгоритмические проблемы. Алгоритмическая неразрешимость. Проблемы самоприменимости и останова для машин Тьюринга

- Основные неразрешимые алгоритмические проблемы теории ЧРФ. Полувычислимые проблемы

- Примечательные неразрешимые проблемы математики

- Временная и емкостная сложность машины Тьюринга. Сложность по худшему случаю. Абстрактные меры сложности. Верхняя граница сложности вычислений. Существовании сложновычислимой функции. Теорема Блюма

- Сложность массовой проблемы. Класс сложности «P» и его свойства. Практическая значимость. Примеры лёгкорешаемых и труднорешаемых задач

- Класс «NP»: задача удостоверения, выделение класса «NP», недетерминированная

машина Тьюринга. Взаимосвязь классов«P» и «NP». Полиномиальная сводимость.

- NP-полные и NP-трудные задачи и их свойства. Доказательство NP-полноты. Теорема Кука

- Примеры NP-полных задач. Сильная NP-полнота.

8.3.6. Ресурсы АПИМ УрФУ, СКУД УрФУ для проведения тестового контроля в рамках текущей и промежуточной аттестации

не используются

8.3.7. Ресурсы ФЭПО для проведения независимого тестового контроля

не используются

8.3.8. Интернет-тренажеры

не используются