**МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ**

Федеральное государственное бюджетное образовательное учреждение высшего образования «Московский государственный университет имени М.В.Ломоносова»

«Утверждаю»

Декан факультета ВМК МГУ
имени М.В. Ломоносова

академик _____ Е.И. Моисеев

# РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

«Совместная разработка вычислительных алгоритмов и вычислительных архитектур»

Уровень высшего образования – подготовка научно-педагогических кадров в аспирантуре

Направление подготовки – 09.06.01 Информатика и вычислительная техника.

Направленность (профиль) – 05.13.11 Математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей.

2018

## РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

### 1. НАИМЕНОВАНИЕ ДИСЦИПЛИНЫ

Совместная разработка вычислительных алгоритмов и вычислительных архитектур.

### 2. УРОВЕНЬ ВЫСШЕГО ОБРАЗОВАНИЯ

Подготовка научно-педагогических кадров в аспирантуре.

### 3. НАПРАВЛЕНИЕ ПОДГОТОВКИ, НАПРАВЛЕННОСТЬ (ПРОФИЛЬ) ПОДГОТОВКИ

Направление подготовки – 09.06.01 Информатика и вычислительная техника. Направленность (профиль) – Математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей.

### 4. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОСНОВНОЙ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина относится к специальным дисциплинам вариативной части образовательной программы и является обязательной для освоения.

### 5. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ

Дисциплина участвует в формировании следующих компетенций образовательной программы:

| Формируемые компетенции | Планируемые результаты обучения |
|---|---|

| | |
|---|---|
| Владением методологией теоретических и экспериментальных исследований в области профессиональной деятельности<br><br>(ОПК-1) | З1 (ОПК-1) ЗНАТЬ:<br>современные математические методы, применяющиеся для решения задач в области естественных наук, экономики, социологии и информационно-коммуникационных технологий<br>У1 (ОПК-1) УМЕТЬ:<br>применять современные методы постановки и анализа задач в области математики и информатики<br>В1 (ОПК-1) ВЛАДЕТЬ:<br>навыками оптимального выбора современных методов и средств постановки и анализа задач в области математики и информатики |
| Способность разрабатывать и реализовывать алгоритмы организации работы современных вычислительных комплексов и компьютерных сетей<br>(ПК-2) | З1(ПК-2) ЗНАТЬ:<br>классические методы разработки и реализации алгоритмов организации работы вычислительных комплексов и компьютерных сетей;<br>УМЕТЬ:<br>применять классические методы разработки и реализации алгоритмов организации работы вычислительных комплексов и компьютерных сетей;<br>ВЛАДЕТЬ:<br>базовыми навыками выбора методов разработки и реализации алгоритмов организации работы вычислительных комплексов и компьютерных сетей. |

| | |
|---|---|
| Способность к реализации различных математических алгоритмов в виде программных комплексов, ориентированных на современную вычислительную технику<br>(ПК-4) | З1( ПК-4) ЗНАТЬ:<br>классические методы реализации различных математических алгоритмов в виде программных комплексов;<br>У1(ПК-4) УМЕТЬ:<br>применять классические методы реализации различных математических алгоритмов в виде программных комплексов;<br>В1 (ПК-4) ВЛАДЕТЬ:<br>базовыми навыками выбора методов реализации различных математических алгоритмов в виде программных комплексов. |

Оценочные средства для промежуточной аттестации приведены в Приложении.

## 6. ОБЪЕМ ДИСЦИПЛИНЫ

Объем дисциплины составляет 3 зачетных единицы, всего 108 часов.

40 часов составляет контактная работа с преподавателем – 32 часа занятий лекционного типа, 0 часов занятий семинарского типа (семинары, научно-практические занятия, лабораторные работы и т.п.), 0 часов индивидуальных консультаций, 4 часа мероприятий текущего контроля успеваемости, 2 часа групповых консультаций, 2 часа мероприятий промежуточной аттестации.

68 часов составляет самостоятельная работа аспиранта.

## 7. ВХОДНЫЕ ТРЕБОВАНИЯ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Учащиеся должны владеть знаниями по операционным системам, прикладному и системному программированию, численным методам, соответствующими основным образовательным программам бакалавриата и магистратуры по укрупненным группам направлений и специальностей 01.00.00 «Математика и механика», 02.00.00 «Компьютерные и информационные науки».

## 8. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

В процессе обучения используется дистанционный доступ через Интернет к схемотехническому стенду ИПМ им. М.В. Келдыша РАН.

## 9. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

В курсе рассматриваются основные проблемы и задачи вычислительной схемотехники, то есть методов схемной реализации вычислений в FPGA с целью ускорения расчетов. На конкретных примерах показывается, что задача ускорения расчета путем схемной реализации части приложения ни в коей мере не сводится к механическому переписыванию исходного текста вычислительного алгоритма на тот или иной «схемный» язык. Свойства алгоритмов, технологии разработки и свойства "железа" обсуждаются в диалектической взаимосвязи. Проводится систематизация и классификация ограничений на алгоритмы, для ускорения которых пригодны те или иные нетрадиционные вычислительные архитектуры. Формулируется и изучается в программистском приближении схемотехническая модель программирования.

| **Наименование и краткое содержание разделов и тем дисциплины (модуля),**<br><br>**форма промежуточной аттестации по дисциплине (модулю)** | **Всего (часы)** | В том числе | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | **Контактная работа (работа во взаимодействии с преподавателем), часы**<br>из них | | | | | | **Самостоятельная работа обучающегося, часы**<br>из них | | |
| | | Занятия лекционного типа | Занятия семинарского типа | Групповые консультации | Индивидуальные консультации | Учебные занятия, направленные на проведение текущего контроля успеваемости (коллоквиумы, практические контрольные занятия и др)* | **Всего** | Выполнение домашних заданий | Подготовка рефератов и т.п.. | **Всего** |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| **Тема 1. Пригодность алгоритмов к архитектурному ускорению вычислений.**<br>Необходимость в нетрадиционных вычислительных архитектурах. Энергетическая метрика эффективности вычислительной архитектуры. Эффективность вычислителя как эффективность организации происходящих в нем коммуникаций между функциональными устройствами. Необходимость локализации обработки. Удельная вычислительная нагрузка (коэффициент переиспользования адресов). Удельная производительность в расчете на такт.<br><br>Классификация приложений вычислительной линейной алгебры с точки зрения возможности локализации обработки, в частности:<br><br>Модельное приложение №1. Сеточный аналог задачи Дирихле для уравнения Пуассона. Однородная прямоугольная сетка. Метод Якоби.<br><br>Модельное приложение №2. Решение СЛАУ с разреженной симметричной матрицей общего вида методом сопряженных градиентов с блочным предобуславливателем Гаусса-Зейделя.<br><br>Примерная классификация методов частиц/квантовой химии/молекулярной динамики.<br><br>Модельное приложение №3: процесс денатурации ДНК. | | | - | - | - | | 7 | 6 | - | 6 |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| **Тема 2. Классификация нефоннеймановских вычислителей и систем на их базе.**<br>Источники ускорения для разных классов. Схемная реализация вычислительных ядер как наиболее радикальный подход к выбору архитектуры сопроцессора - ускорителя.<br>Как устроена аппаратура внутри: четыре шага "сотворения цифрового мира". Программистская, схемотехническая и радиоэлектронная картины мира. Глубинное родство схемотехники и параллельного программирования.<br>Роль длинных синхронных конвейеров в схемном ускорении счета. Необходимость адекватных языков описания логики схем. | 10 | 2 | - | - | - | - | 2 | 2 | 6 | 8 |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| **Тема 3. Технология схемной реализации вычислительных ядер в примерах и задачах.**<br>Подготовительная реорганизация исходных текстов. Программная модель канала связи процессора с сопроцессором. Структурно выделенная программная модель сопроцессора как задание на его (сопроцессора) разработку.<br>Недостаточность традиционного языка для описания схемной реализации сопроцессора. Недостаточность программистской картины мира для использования нетрадиционных языков. Два способа закрыть разрыв, в частности:<br>- система программирования Vivado HLS от Xilinx;<br>- система программирования Автокод Stream от ИПМ РАН.<br>Базовый слой языка Автокод как попытка прямого и явного выражения схемотехнической программистской модели (в отличие от непрямого и косвенного ее выражения в языках VHDL и Verilog).<br>Сравнение двух технологий разработки сопроцессора в рамках единой методики структурной подготовки программы - на примерах модельных приложений №1 и №3. | 15 | 8 | - | - | - | 1 | 9 | 6 | - | 6 |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| **Тема 4. Сочетание разнородных инструментов описания логики вычислительных схем в одном проекте.**<br><br>Примеры несостоятельности компилятора Vivado HLS при построении длинных синхронных конвейеров. Стиль программирования, позволяющий преодолеть некоторые трудности. Необходимость точечного использования низкоуровневых инструментов для преодоления остальных. Сложность вставки инородной логики в схему, построенную компилятором. Синхронные и асинхронные вставки. | 9 | 4 | - | - | - | 1 | 5 | 4 | - | 4 |
| **5. Промежуточная аттестация – устный экзамен** | 38 | 2 | | | | | | 36 | | |
| **Итого** | 108 | 40 | | | | | | 68 | | |

## 10. УЧЕБНО-МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ УЧАЩИХСЯ

Самостоятельная работа учащихся состоит в изучении лекционного материала, учебно-методической литературы, подготовки к текущему контролю и промежуточной аттестации.

Литература для самостоятельной работы студентов в соответствии с тематическим планом .

**Тема 1 «Пригодность алгоритмов к архитектурному ускорению вычислений»**

1. А.О. Лацис, В.К. Левин, Перспективы развития суперкомпьютерной техники (по материалам лекции 27.08.2012, Дубна, MPAMCS-2012), Матем. моделирование, 2013, том 25, номер 11, 128–136

http://www.mathnet.ru/links/cdb1de25634456b2b2ff3a1c9b46a7c2/mm3424.pdf

2. P. Kogge. Next-Generation Supercomputers.

https://spectrum.ieee.org/computing/hardware/nextgeneration-supercomputers. Дата обращения 09.10.2017г. Загруженная страница прилагается.

3. С.С. Андреев, С.А. Дбар, А.О. Лацис, Е.А. Плоткина. Как и почему могут быть использованы на практике суперкомпьютеры на базе FPGA. М., РАН, 2017. ISBN 978-5-906906-61-8.

http://www.ras.ru/FStorage/Download.aspx?id=9001855c-3ec6-4c70-b259-d25a50c20298

**Тема 2 «Классификация не-фоннеймановских вычислителей и систем на их базе»**

1. Деммель Дж. Вычислительная линейная алгебра. Теория и приложения
2. http://www.netlib/org/templates/templates.pdf
3. С.С. Андреев, С.А. Дбар, А.О. Лацис, Е.А. Плоткина. О новых архитектурах и новых тестах производительности. Тезисы докладов 20-й всероссийской конференции "Теоретические основы и конструирование численных алгоритмов решения задач математической физики", посвященной памяти К.И. Бабенко. Дюрсо, 2014, с. 17-18.

**Тема 3 «Технология схемной реализации вычислительных ядер в примерах и задачах»**

1. Лацис А.О. Параллельная обработка данных.

2. NVIDIA Accelerated Computing. CUDA Zone. https://developer.nvidia.com/cuda-zone Дата обращения 09.10.2017г.

**Тема 4 «Сочетание разнородных инструментов описания логики вычислительных схем в одном проекте»**

## 11. РЕСУРСНОЕ ОБЕСПЕЧЕНИЕ

Личные компьютеры обучающихся с возможностью выхода в Интернет.

**Основная литература**

**1.** Разработка высокопроизводительных массово-параллельных гибридных вычислителей и способов их применения. http://kiam.ru/MVS/research/faq.html

**2.** Андреев С. С., Дбар С. А., Лацис А. О., Плоткина Е. А. Инженер-
ная методика адаптации приложения к гибридному кластеру с ускорителями на ПЛИС. http://kiam.ru/MVS/research/fpga/ingmet/ .

**Дополнительная литература**

1. Андреев С. С., Дбар С. А., Лацис А. О., Плоткина Е. А. Гибридный реконфигурируемый вычислитель. Руководство программиста на языке Автокод. http://kiam.ru/MVS/research/fpga/progman.

2. Андреев С. С., Дбар С. А., Лацис А. О., Плоткина Е. А. Схемотехнический стенд mvse.kiam.ru Руководство пользователя.

http://kiam.ru/MVS/research/fpga/userman.html.

**Ресурсы информационно-телекоммуникационной сети «Интернет»**

http://elibrary.ru
www.scopus.com

**Материально-техническая база**

Для преподавания дисциплины требуется класс, оборудованный маркерной или меловой доской и проектором.

## 12. ЯЗЫК ПРЕПОДАВАНИЯ

Русский

## 13. РАЗРАБОТЧИК ПРОГРАММЫ, ПРЕПОДАВАТЕЛИ

профессор, д.ф.-м.н. Лацис Алексей Оттович

**Приложение**

## ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ

««Совместная разработка вычислительных алгоритмов и вычислительных архитектур»

Средства для оценивания планируемых результатов обучения, критерии и показатели оценивания приведены ниже.

| **РЕЗУЛЬТАТ ОБУЧЕНИЯ по дисциплине (модулю)** | **КРИТЕРИИ и ПОКАЗАТЕЛИ ОЦЕНИВАНИЯ РЕЗУЛЬТАТА ОБУЧЕНИЯ по дисциплине (модулю)** *(критерии и показатели берутся из соответствующих карт компетенций, при этом пользуются либо традиционной системой оценивания, либо БРС)* | | | | | **ОЦЕНОЧНЫЕ СРЕДСТВА** |
|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 | |
| | **Неудовлетворительно** | **Неудовлетворительно** | **Удовлетворительно** | **Хорошо** | **Отлично** | |
| ЗНАТЬ: современные математические методы, применяющиеся для решения задач в области естественных наук, экономики, социологии и информационно-коммуникационных технологий **Код З1 (ОПК-1)** | Отсутствие знаний | Фрагментарные представления о современных математических методах, применяющихся для решения задач в области естественных наук, экономики, социологии и информационно-коммуникационных технологий | В целом сформированные, но неполные знания о современных математических методах, применяющихся для решения задач в области естественных наук, экономики, социологии и информационно-коммуникационных технологий | Сформированные, но содержащие отдельные пробелы знания о современных математических методах, применяющихся для решения задач в области естественных наук, экономики, социологии и информационно-коммуникационных технологий | Сформированные систематические знания о современных математических методах, применяющихся для решения задач в области естественных наук, экономики, социологии и информационно-коммуникационных технологий | Устный экзамен |

| | | | | | | |
|---|---|---|---|---|---|---|
| УМЕТЬ:<br>применять современные методы постановки и анализа задач в области математики и информатики<br>**Код У1 (ОПК-1)** | Отсутствие умений | Фрагментарные умения применять современные методы постановки и анализа задач в области математики и информатики | В целом успешное, но не систематическое умение применять современные методы постановки и анализа задач в области математики и информатики | Успешное, но содержащее отдельные пробелы умение применять современные методы постановки и анализа задач в области математики и информатики | Сформированное умение применять современные методы постановки и анализа задач в области математики и информатики | Устный экзамен |
| ВЛАДЕТЬ:<br>навыками оптимального выбора современных методов и средств постановки и анализа задач в области математики и информатики<br>**Код В1 (ОПК-1)** | Отсутствие навыков | Фрагментарное владение навыками оптимального выбора современных методов и средств постановки и анализа задач в области математики и информатики | В целом успешное, но не полное владение навыками оптимального выбора современных методов и средств постановки и анализа задач в области математики и информатики | Успешное, но содержащее отдельные пробелы владение навыками оптимального выбора современных методов и средств постановки и анализа задач в области математики и информатики | Сформированное владение навыками оптимального выбора современных методов и средств постановки и анализа задач в области математики и информатики | Устный экзамен |
| ЗНАТЬ:<br>современные методы разработки и реализации алгоритмов организации работы вычислительных комплексов и компьютерных сетей последнего поколения<br>**Код З1 (ПК-2)** | Отсутствие знаний | Фрагментарные представления о современных методах разработки и реализации алгоритмов организации работы вычислительных комплексов и компьютерных сетей последнего поколения | В целом сформированные, но неполные знания о современных методах разработки и реализации алгоритмов организации работы вычислительных комплексов и компьютерных сетей последнего поколения | Сформированные, но содержащие отдельные пробелы знания о современных методах разработки и реализации алгоритмов организации работы вычислительных комплексов и компьютерных сетей последнего поколения | Сформированные систематические знания о современных методах разработки и реализации алгоритмов организации работы вычислительных комплексов и компьютерных сетей последнего поколения | Устный экзамен |

| | | | | | | |
|---|---|---|---|---|---|---|
| УМЕТЬ:<br>применять современные методы разработки и реализации алгоритмов организации работы вычислительных комплексов и компьютерных сетей последнего поколения<br>**Код У1 (ПК-2)** | Отсутствие умений | Фрагментарные умения применять современные методы разработки и реализации алгоритмов организации работы вычислительных комплексов и компьютерных сетей последнего поколения | В целом успешное, но не систематическое умение применять современные методы разработки и реализации алгоритмов организации работы вычислительных комплексов и компьютерных сетей последнего поколения | Успешное, но содержащее отдельные пробелы умение применять современные методы разработки и реализации алгоритмов организации работы вычислительных комплексов и компьютерных сетей последнего поколения | Сформированное умение применять современные методы разработки и реализации алгоритмов организации работы вычислительных комплексов и компьютерных сетей последнего поколения | Отчет |
| ВЛАДЕТЬ:<br>навыками оптимального выбора современных методов разработки и реализации алгоритмов организации работы вычислительных комплексов и компьютерных сетей последнего поколения<br>**Код В1 (ПК-2)** | Отсутствие навыков | Фрагментарное владение навыками оптимального выбора современных методов разработки и реализации алгоритмов организации работы вычислительных комплексов и компьютерных сетей последнего поколения | В целом успешное, но не полное владение навыками оптимального выбора современных методов разработки и реализации алгоритмов организации работы вычислительных комплексов и компьютерных сетей последнего поколения | Успешное, но содержащее отдельные пробелы владение навыками оптимального выбора современных методов разработки и реализации алгоритмов организации работы вычислительных комплексов и компьютерных сетей последнего поколения | Сформированное владение навыками оптимального выбора современных методов разработки и реализации алгоритмов организации работы вычислительных комплексов и компьютерных сетей последнего поколения | Отчет |

| | | | | | | |
|---|---|---|---|---|---|---|
| ЗНАТЬ:<br>современные методы реализации различных математических алгоритмов в виде программных комплексов, особенности современных вычислительных комплексов<br>**Код З1 (ПК-4)** | Отсутствие знаний | Фрагментарные представления о современных методах реализации различных математических алгоритмов в виде программных комплексов, особенностях современных вычислительных комплексов | В целом сформированные, но неполные знания о современных методах реализации различных математических алгоритмов в виде программных комплексов, особенностях современных вычислительных комплексов | Сформированные, но содержащие отдельные пробелы знания о современных методах реализации различных математических алгоритмов в виде программных комплексов, особенностях современных вычислительных комплексов | Сформированные систематические знания о современных методах реализации различных математических алгоритмов в виде программных комплексов, особенностях современных вычислительных комплексов | Устный экзамен |
| УМЕТЬ:<br>применять современные методы реализации различных математических алгоритмов в виде программных комплексов с учетом особенностей современных вычислительных комплексов<br>**Код У1 (ПК-4)** | Отсутствие умений | Фрагментарные умения применять современные методы реализации различных математических алгоритмов в виде программных комплексов с учетом особенностей современных вычислительных комплексов | В целом успешное, но не систематическое умение применять современные методы реализации различных математических алгоритмов в виде программных комплексов с учетом особенностей современных вычислительных комплексов | Успешное, но содержащее отдельные пробелы умение применять современные методы реализации различных математических алгоритмов в виде программных комплексов с учетом особенностей современных вычислительных комплексов | Сформированное умение применять современные методы реализации различных математических алгоритмов в виде программных комплексов с учетом особенностей современных вычислительных комплексов | Отчет |

| | | | | | | |
|---|---|---|---|---|---|---|
| ВЛАДЕТЬ:<br>навыками оптимального выбора и создания новых современных методов реализации математических алгоритмов в виде программных комплексов, учитывающих особенности современных вычислительных комплексов<br>**Код В1 (ПК-4)** | Отсутствие навыков | Фрагментарное владение навыками оптимального выбора и создания новых современных методов реализации математических алгоритмов в виде программных комплексов, учитывающих особенности современных вычислительных комплексов | В целом успешное, но не полное владение навыками оптимального выбора и создания новых современных методов реализации математических алгоритмов в виде программных комплексов, учитывающих особенности современных вычислительных комплексов | Успешное, но содержащее отдельные пробелы владение навыками оптимального выбора и создания новых современных методов реализации математических алгоритмов в виде программных комплексов, учитывающих особенности современных вычислительных комплексов | Сформированное владение навыками оптимального выбора и создания новых современных методов реализации математических алгоритмов в виде программных комплексов, учитывающих особенности современных вычислительных комплексов | Отчет |

**Фонды оценочных средств, необходимые для оценки результатов обучения**

Список вопросов для устного экзамена.

1. Особенности современных автоматизированных систем.
2. Требования к системам и средствам защиты информации от несанкционированного доступа.
3. Классификация автоматизированных систем и требования по защите информации.
4. Показатели защищенности средств вычислительной техники.
5. Соответствие классов систем различным уровням конфиденциальности.
6. Понятие модели нарушителя информационной безопасности и модели угроз информационной безопасности.
7. Политика безопасности.
8. Принципы построения системы защиты информации.
9. Определение уязвимостей автоматизированных систем и выбор средств защиты.
10. Формирование требований к построению систем защиты.
11. Создание автоматизированных систем в защищенном исполнении.

12. Классификация каналов утечки информации.
13. Методы защиты речевой информации.
14. Методы защиты информации от утечки за счет побочных электромагнитных излучений и наводок.
15. Специальные проверки и специальные исследования оборудования.
16. Противодействие наблюдению в оптическом диапазоне.
17. Инженерно-техническая защита информации.
18. Методы противодействия разведкам.
19. Методы контроля доступа к ресурсам компьютерной системы.
20. Модели безопасности компьютерных систем.
21. Дискреционные модели безопасности: модель Харрисона-Рузо-Ульмана.
22. Модель типизированных матриц доступа.
23. Модель take-grant.
24. Мандатное управление доступом.
25. Модель Белла-Лападулы.
26. Модель LWM.
27. Автоматная модель невлияния.
28. Методы поиска остаточной информации на машинных носителях.
29. Методы гарантированного удаления информации.
30. Сущность разрушающих программных воздействий.
31. Модели взаимодействия прикладных программ и программы-злоумышленника, классификация разрушающих программных средств.
32. Компьютерные вирусы. Принципы и методы защиты от разрушающих программных воздействий.
33. Уязвимости приложений: атаки типа переполнение буфера, стека и кучи, атаки, основанные на изменении входных данных.
34. Атаки на web-приложения: атаки типа SQL-инъекция и межсайтовый скриптинг.
35. Безопасность сокетов.
36. Безопасность ActiveX-элементов, DCOM-объектов и RPC-элементов.
37. Атаки типа «отказ в обслуживании».
38. Требования ФСТЭК России к программному обеспечению средств защиты и его классификация по уровню отсутствия недекларированных возможностей.
39. Виртуальные частные сети. Криптографическая защита трафика на всех уровнях модели ISO/OSI.
40. Криптографическая защиты сетевого уровня. Семейство протоколов IPsec и его модификации.

41. Средства криптографической защиты прикладного уровня. Протокол SSL/TLS.
42. Протокол RADIUS, протокол Kerberos.
43. Проблема разграничения доступа в компьютерных сетях. Понятие межсетевого экрана.
44. Виды межсетевых экранов. Принципы работы межсетевых экранов.
45. Уязвимости основных протоколов сетевого взаимодействия.
46. Понятие системы обнаружения вторжений и ее функции. Основные методы детектирования атак.

Материалы для мероприятий текущего контроля.

Мероприятия текущего контроля реализуются в виде тестов с выбором вариантов ответа. Четыре набора тестов охватывают теоретический материал, относящийся соответственно к темам 1, 3, 4 и 5. Вопросы тестов соответствуют приведенным выше вопросам к устному экзамену, раскрывая их на более подробном уровне.

Примерные темы рефератов.

Реферат посвящен Теме 2. Примеры тем:

- Методические подходы к оценке эффективности защиты речевой информации.
- Электромагнитные низкочастотные каналы утечки информации.
- Маскирование сигналов шумами, коррелированными с сигналами.
- Задачи контроля каналов утечки информации в реальном масштабе времени.

## Методические материалы для проведения процедур оценивания результатов обучения

**Особенности организации процесса обучения**

Для эффективного освоения курса рекомендуется перед каждым занятие привести в порядок конспекты лекций. После каждого заня-

тия рекомендуется найти и прочитать дополнительную литературу по теме лекции и прочитать свои конспекты.

**Система контроля и оценивания**

За каждую контрольную работу и реферат выставляются баллы (максимум 10 баллов за каждый вид работы). Пусть М – максимальное число баллов, которое может набрать студент. В конце семестра баллы конвертируются в оценку О1 следующим образом:

меньше М/2 баллов: О1=2;

больше или равно М/2 баллов, но меньше 2М/3: О1=3;

больше или равно 2М/3 баллов, но меньше 5М/6: О1=4;

больше или равно 5М/6 баллов: О1=5.

На экзамене оценка О1 является стартовой. Окончательная оценка определяется исходя из оценки устного ответа студента, при этом она не может отличаться от стартовой оценки более чем на 1 балл.

**Структура и график контрольных мероприятий**

Контрольная работа на 3-й, 8-й, 10-й, 14-й неделях, реферат в течение семестра, устный экзамен в конце семестра.