

АВТОНОМНАЯ НЕКОММЕРЧЕСКАЯ ОБРАЗОВАТЕЛЬНАЯ
ОРГАНИЗАЦИЯ ВЫСШЕГО ОБРАЗОВАНИЯ
ЦЕНТРОСОЮЗА РОССИЙСКОЙ ФЕДЕРАЦИИ
«РОССИЙСКИЙ УНИВЕРСИТЕТ КООПЕРАЦИИ»
КАЗАНСКИЙ КООПЕРАТИВНЫЙ ИНСТИТУТ (ФИЛИАЛ)

Среднее профессиональное образование

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Специальность

09.02.05 Прикладная информатика (по отраслям)

Квалификация выпускника:

Техник-программист

Казань 2019

Рабочая программа учебной дисциплины «Информационная безопасность» (для 2019 года набора) разработана на основе Федерального государственного образовательного стандарта среднего профессионального образования по специальности 09.02.05 Прикладная информатика (по отраслям), утвержденного Министерством образования и науки Российской Федерации от 13 августа 2014 г. № 1001 и учебного плана, утвержденного Ученым советом Российского университета кооперации

Разработчики:

Ахмедова А.М., доцент кафедры естественных дисциплин, сервиса и туризма Казанского кооперативного института (филиала) Российского университета кооперации

Рабочая программа:

обсуждена и рекомендована к утверждению решением кафедры естественных дисциплин, сервиса и туризма Казанского кооперативного института (филиала) от 13.03.2019, протокол № 7

одобрена Научно-методическим советом Казанского кооперативного института (филиала) от 03.04.2019, протокол №5

утверждена Ученым советом Российского университета кооперации от 18.04.2019, протокол №4

© Казанский кооперативный институт (филиал) Российского университета кооперации, 2019
© Ахмедова А.М., 2019

СОДЕРЖАНИЕ

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»	4
1.1. Область применения программы	4
1.2. Место дисциплины в структуре основной профессиональной образовательной программы.....	4
1.3.Цель и задачи учебной дисциплины – требования к результатам освоения учебной дисциплины	4
1.4. Количество часов на освоение рабочей программы учебной дисциплины (по ФГОС):	6
2 СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ.....	6
2.1 Объем учебной дисциплины и виды учебной работы.....	6
2.2 Тематический план и содержание учебной дисциплины «Информационная безопасность»	7
3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ДИСЦИПЛИНЫ	12
3.1. Требования к минимальному материально-техническому обеспечению	12
3.2. Информационное обеспечение обучения	12
4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ДИСЦИПЛИНЫ	13

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

1.1. Область применения программы

Учебная дисциплина «Информационная безопасность» является частью программы подготовки специалистов среднего звена в соответствии с Федеральным государственным образовательным стандартом от 13.08.2014 г. №1001, и учебным планом, утвержденным Ученым советом Российского университета кооперации по специальности СПО 09.02.05 Прикладная информатика (по отраслям).

1.2. Место дисциплины в структуре основной профессиональной образовательной программы

Учебная дисциплина «Информационная безопасность» относится к общепрофессиональным дисциплинам профессионального цикла.

1.3. Цель и задачи учебной дисциплины – требования к результатам освоения учебной дисциплины

В результате изучения дисциплины обучающийся должен:

уметь:

- проводить анализ и оценку уязвимостей компьютерной системы;
- применять меры информационной безопасности процедурного уровня.
- осуществлять защиту информации от несанкционированного доступа.
- настраивать безопасность почтового клиента;
- настраивать параметры аутентификации пользователей;
- осуществлять регистрацию и аудит информационной безопасности;
- настраивать системы разграничения доступа;
- применять криптографические методы и средства защиты информации;
- использовать средства антивирусной защиты;
- использовать стандарты и спецификации информационной безопасности;
- определять оптимальную конфигурацию оборудования и характеристик устройств для конкретных задач;
- идентифицировать основные узлы персонального компьютера, разъемы для подключения внешних устройств;
- обеспечивать совместимость аппаратных и программных средств вычислительной техники.

знать:

- понятие и составляющие информационной безопасности;
- виды угроз информации и методы защиты от них;

- законы, стандарты и спецификации информационной безопасности;
- меры процедурного уровня информационной безопасности;
- меры программно-технического уровня информационной безопасности;
- методы защиты информации от несанкционированного доступа;
- способы разграничения полномочий и доступа к объектам;
- осуществление регистрации и аудита в компьютерной системе;
- проведение оценки рисков компьютерной системы;
- применение средств антивирусной защиты.
- построение цифровых вычислительных систем и их архитектурные особенности;
- принципы работы основных логических блоков системы;
- параллелизм и конвейеризацию вычислений;
- классификацию вычислительных платформ;
- принципы вычислений в многопроцессорных и многоядерных системах;
- принципы работы кэш-памяти;
- методы повышения производительности многопроцессорных и многоядерных систем;
- основные энергосберегающие технологии.

Учебная дисциплина «Информационная безопасность» обеспечивает формирование профессиональных и общих компетенций:

ОК 1. Понимать сущность и социальную значимость своей будущей профессии, проявлять к ней устойчивый интерес.

ОК 2. Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество.

ОК 3. Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность.

ОК 4. Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития.

ОК 5. Использовать информационно-коммуникационные технологии в профессиональной деятельности.

ОК 6. Работать в коллективе и команде, эффективно общаться с коллегами, руководством, потребителями.

ОК 7. Брать на себя ответственность за работу членов команды (подчиненных), результат выполнения заданий.

ОК 8. Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации.

ОК 9. Ориентироваться в условиях частой смены технологий в профессиональной деятельности.

ПК 2.1. Осуществлять сбор и анализ информации для определения потребностей клиента.

ПК 2.2 Разрабатывать и публиковать программное обеспечение и информационные ресурсы отраслевой направленности со статическим и динамическим контентом на основе готовых спецификаций и стандартов.

ПК 2.5 Разрабатывать и вести проектную и техническую документацию.

ПК 2.6 Участвовать в измерении и контроле качества продуктов.

ПК 3.4 Работать с системами управления взаимоотношениями с клиентами.

1.4. Количество часов на освоение рабочей программы учебной дисциплины (по ФГОС):

	Очная форма	Заочная форма
Максимальная учебная нагрузка обучающегося:	46	46
- обязательная аудиторная учебная нагрузка	34	10
- самостоятельная работа обучающегося	12	36

2 СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

2.1 Объем учебной дисциплины и виды учебной работы

очная форма обучения

Вид учебной работы	Объем часов
Максимальная учебная нагрузка (всего)	46
Обязательная аудиторная учебная нагрузка (всего)	34
в том числе: теоретическое обучение	12
Лабораторные занятия	22
Самостоятельная работа обучающегося (всего)	12
Промежуточная аттестация (8 семестр) на базе основного общего образования (7 семестр) на базе среднего общего образования	Зачет

заочная форма обучения

Вид учебной работы	Объем часов
Максимальная учебная нагрузка (всего)	46
Обязательная аудиторная учебная нагрузка (всего)	10
в том числе: теоретическое обучение	4
Лабораторные занятия	6
Самостоятельная работа обучающегося (всего)	36
Промежуточная аттестация (4 курс) на базе основного общего образования	Зачет

2.2 Тематический план и содержание учебной дисциплины «Информационная безопасность»

очная форма обучения

Наименование разделов и тем	Содержание учебного материала, практических занятий, самостоятельная работа обучающихся	Объем часов	Уровень освоения
<i>1</i>	<i>2</i>	<i>3</i>	<i>4</i>
Тема 1.1. Общие проблемы безопасности, роль и место информационной безопасности	Содержание учебного материала Национальные интересы и безопасность Информационная безопасность Защита информации (ЗИ)	2	1
	Самостоятельная работа обучающегося Реферат по теме «История становления национальной безопасности страны» «Виды угроз информационной безопасности Российской Федерации».	2	3
Тема 1.2. Защита информации в автоматизированных системах обработки данных	Содержание учебного материала Предмет и объекты защиты информации в автоматизированных системах обработки данных (АСОД) Элементы и объекты защиты в АСОД Функции и задачи защиты информации Методы и системы защиты информации	2	1
	Лабораторное занятие 1.Лабораторная работа Защита документов, созданных в Microsoft Word. 2.Лабораторная работа Защита документов, созданных в Microsoft Excel.	4	2
	Самостоятельная работа обучающегося Составление блок-схемы «Классификация защищаемой информации по видам тайн». Написание реферата на тему «Информационная война».	2	3
Тема 1.3. Криптографические методы защиты информации	Содержание учебного материала Криптология и основные этапы ее развития Методы криптографического преобразования данных. Проблемы реализации методов криптографической защиты в АСОД	2	1
	Лабораторное занятие 3.Лабораторная работа «Шифры и криптоанализ», «Шифрование и дешифрование информации с использованием шифров перестановки и простой замены», «Шифрование и дешифрование информации с использованием схемы Вижинера» 4.Лабораторная работа «Закрытый ключ электронной цифровой подписи», «Открытый ключ электронной цифровой подписи», «Сертификат ключа подписи».	4	2

	<p>Самостоятельная работа обучающегося Составление конспекта по теме «Шифр Цезаря: история возникновения, алгоритм шифрования и дешифрования информации». «Составление электронной презентации «Биография Блеза де Вижинера».</p>	2	3
<p>Тема 1.4. Защита информации в персональных компьютерах</p>	<p>Содержание учебного материала Особенности защиты информации в персональных ЭВМ Защита ПК от несанкционированного доступа Вредоносные закладки в ПК и борьба с ними</p>	2	1
	<p>Лабораторное занятие 5. Защита документов, созданных в Microsoft Access. Защита файла паролем 6. Изучение особенностей применения современных специализированных пакетов антивирусных программ и приложений</p>	6	2
	<p>Самостоятельная работа обучающегося Создание электронной презентации на тему «Программы для раскрытия пароля». Написание реферата «Образцы технических средств обеспечения информационной и общей безопасности».</p>	2	3
<p>Тема 1.5. Компьютерные вирусы и антивирусные программы.</p>	<p>Содержание учебного материала Компьютерный вирус Методы защиты. Антивирусы Некоторые примеры антивирусных программ</p>	2	1
	<p>Лабораторное занятие 8.Лабораторная работа Классификация компьютерных вирусов. 9.Лабораторная работа Защита ПК от вредоносных закладок (разрушающих программных средств)</p>	4	2
	<p>Самостоятельная работа обучающегося Создание электронной презентации «История возникновения компьютерных вирусов». Составление конспекта по теме «Признаки заражения компьютера». Составление блок-схемы «Классификация вредоносных программ». Составление блок-схемы «Классификация антивирусных программ». Составление конспекта по теме «Основные принципы работы антивирусной программы NOD 32».</p>	2	3

Тема 1.6. Проблемы защиты информации в сетях ЭВМ. Технические средства и комплексное обеспечение безопасности	Содержание учебного материала Сети ЭВМ — построение и использование Цели, функции и задачи защиты информации в сетях ЭВМ Архитектура механизмов защиты информации в сетях ЭВМ Технические средства защиты Комплексный подход к обеспечению безопасности.	2	1
	Лабораторное занятие 10.Лабораторная работа « Особенности защиты информации в базах данных »	4	2
	Самостоятельная работа обучающегося Противодействие несанкционированному межсетевому доступу. Создание буклета на тему «Документы, регламентируемые деятельность в области защиты информации». Составление сравнительной таблицы «Отечественные и зарубежные стандарты в области информационной безопасности». Контрольная работа	2	3
Итого часов по дисциплине 46		12/22/12	

заочная форма обучения

Наименование разделов и тем	Содержание учебного материала, практических занятий, самостоятельная работа обучающихся	Объем часов	Уровень освоения
<i>1</i>	<i>2</i>	<i>3</i>	<i>4</i>
Тема 1.1. Общие проблемы безопасности, роль и место информационной безопасности	Содержание учебного материала Национальные интересы и безопасность Информационная безопасность Защита информации (ЗИ)	2	1
	Самостоятельная работа обучающегося Реферат по теме «История становления национальной безопасности страны» «Виды угроз информационной безопасности Российской Федерации».	2	3
Тема 1.2. Защита информации в автоматизированных системах обработки данных	Содержание учебного материала Предмет и объекты защиты информации в автоматизированных системах обработки данных (АСОД) Элементы и объекты защиты в АСОД Функции и задачи защиты информации Методы и системы защиты информации	2	1

	<p>Лабораторное занятие 1.Лабораторная работа Защита документов, созданных в Microsoft Word. 2.Лабораторная работа Защита документов, созданных в Microsoft Excel.</p>	6	2
	<p>Самостоятельная работа обучающегося Составление блок-схемы «Классификация защищаемой информации по видам тайн». Написание реферата на тему «Информационная война».</p>	2	3
<p>Тема 1.3. Криптографические методы защиты информации</p>	<p>Самостоятельная работа обучающегося Криптология и основные этапы ее развития Методы криптографического преобразования данных. Проблемы реализации методов криптографической защиты в АСОД</p>	2	3
	<p>Лабораторная работа «Шифры и криптоанализ», «Шифрование и дешифрование информации с использованием шифров перестановки и простой замены», «Шифрование и дешифрование информации с использованием схемы Вижинера» Лабораторная работа «Закрытый ключ электронной цифровой подписи», «Открытый ключ электронной цифровой подписи», «Сертификат ключа подписи».</p>	4	
	<p>Составление конспекта по теме «Шифр Цезаря: история возникновения, алгоритм шифрования и дешифрования информации». «Составление электронной презентации «Биография Блеза де Вижинера».</p>	2	
<p>Тема 1.4. Защита информации в персональных компьютерах</p>	<p>Самостоятельная работа обучающегося Особенности защиты информации в персональных ЭВМ Защита ПК от несанкционированного доступа Вредоносные закладки в ПК и борьба с ними</p>	2	3
	<p>Защита документов, созданных в Microsoft Access. Защита файла паролем Изучение особенностей применение современных специализированных пакетов антивирусных программ и приложений</p>	4	
	<p>Создание электронной презентации на тему «Программы для раскрытия пароля». Написание реферата «Образцы технических средств обеспечения информационной и общей безопасности».</p>	2	
<p>Тема 1.5. Компьютерные вирусы и антивирусные программы.</p>	<p>Самостоятельная работа обучающегося Компьютерный вирус Методы защиты. Антивирусы Некоторые примеры антивирусных программ</p>	2	3
	<p>Лабораторная работа Классификация компьютерных вирусов. Лабораторная работа Защита ПК от вредоносных закладок (разрушающих программных средств)</p>	4	

	Создание электронной презентации «История возникновения компьютерных вирусов». Составление конспекта по теме «Признаки заражения компьютера». Составление блок-схемы «Классификация вредоносных программ». Составление блок-схемы «Классификация антивирусных программ». Составление конспекта по теме «Основные принципы работы антивирусной программы NOD 32».	2	
Тема 1.6. Проблемы защиты информации в сетях ЭВМ. Технические средства и комплексное обеспечение безопасности	Самостоятельная работа обучающегося Сети ЭВМ — построение и использование Цели, функции и задачи защиты информации в сетях ЭВМ Архитектура механизмов защиты информации в сетях ЭВМ Технические средства защиты Комплексный подход к обеспечению безопасности.	2	3
	Лабораторная работа « Особенности защиты информации в базах данных »	4	
	Противодействие несанкционированному межсетевому доступу. Создание буклета на тему «Документы, регламентируемые деятельность в области защиты информации». Составление сравнительной таблицы «Отечественные и зарубежные стандарты в области информационной безопасности». Контрольная работа	2	
Итого часов по дисциплине 46		4/6/36	

Для характеристики уровня освоения учебного материала используются следующие обозначения:

1. – **ознакомительный** (узнавание ранее изученных объектов, свойств);
2. – **репродуктивный** (выполнение деятельности по образцу, инструкции или под руководством)
3. – **продуктивный** (планирование и самостоятельное выполнение деятельности, решение проблемных задач)

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ДИСЦИПЛИНЫ

3.1. Требования к минимальному материально-техническому обеспечению

Учебная дисциплина реализуется в кабинете *архитектуры электронно-вычислительных машин и вычислительных систем*.

Оборудование учебного кабинета:

Стандартная учебная мебель:

Столы компьютерные;

Столы аудиторные двухместные;

Стулья ученические;

Стул;

Доска аудиторная.

Оборудование, технические средства обучения:

Системные блоки;

Процессоры;

Мониторы;

Клавиатура;

Компьютерные мыши.

Программное обеспечение:

1. Desktop School ALNG LicSAPk MVL.

a. Office ProPlus All Lng Lic/SA Pack MVL Partners in Learning

b. Windows 8/

2. Система тестирования INDIGO.

3. Kaspersky Endpoint Security.

4. Интернет-браузеры Google Chrome, Firefox.

3.2. Информационное обеспечение обучения

Основная литература:

1. Партыка, Т.Л. Информационная безопасность: учебное пособие / Т.Л. Партыка, И.И. Попов, – 5-е изд., перераб. и доп. - М.: Форум, НИЦ ИНФРА-М, 2019. - 432 с. - Режим доступа: <http://znanium.com/catalog/product/987326>

2. Мельников, В.П. Информационная безопасность: учебник / В.П. Мельников, А.И. Куприянов. — Москва : КноРус, 2018. — 267 с. — Для СПО. - Режим доступа: <https://www.book.ru/book/924214>

Дополнительная литература:

1. Ищейнов, В.Я. Основные положения информационной безопасности: учебное пособие / В.Я.Ищейнов, М.В.Мецатунян - М.: Форум, НИЦ ИНФРА-М, 2018. - 208 с. - Режим доступа: <http://znanium.com/catalog.php?bookinfo=927190>

2. Васильков, А.В. Безопасность и управление доступом в

информационных системах [Электронный ресурс]: учебное пособие / А.В. Васильков, И.А. Васильков. - М.: Форум, НИЦ ИНФРА-М, 2019. - 368 с. - Режим доступа: <http://znanium.com/catalog/product/987224>

3. Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей [Электронный ресурс]: учебное пособие / В. Ф. Шаньгин - М.: ИД ФОРУМ, НИЦ ИНФРА-М, 2018. - 416 с. - Режим доступа: <http://znanium.com/catalog/product/945331>

4. Крылов, Г.О. Базовые понятия информационной безопасности [Электронный ресурс]: учеб. пособие / Г.О. Крылов, С.Л. Ларионова, В.Л. Никитина. — Москва : Русайнс, 2017. — 258 с. - Режим доступа: <https://www.book.ru/book/922531>

5. Бабаш, А.В. Информационная безопасность. Лабораторный практикум [Электронный ресурс]: учебное пособие / А.В. Бабаш, Е.К. Баранова, Ю.Н. Мельников. — Москва : КноРус, 2018. — 131 с.- (Бакалавриат). - Режим доступа: <https://www.book.ru/book/926191>

6. Шаханова, М.В. Современные технологии информационной безопасности [Электронный ресурс]: учебно-методическое пособие / М.В. Шаханова. — Москва : Проспект, 2015. — 216 с. - Режим доступа: <https://www.book.ru/book/918747>

7. Основы информационной безопасности [Электронный ресурс]: учебник/ Е.К. Баранова, А.В. Бабаш. - М. : РИОР : ИНФРА-М, 2019. — 202 с. — (Среднее профессиональное образование). — Режим доступа: <http://znanium.com/catalog/product/1014830>

Интернет-ресурсы:

1. Каталог информационной системы «Единое окно доступа к образовательным ресурсам» <http://window.edu.ru/window/catalog> Каталог Российского общеобразовательного портала <http://www.school.edu.ru>

2. Среднее профессиональное образование РФ <http://www.portalspo.ru>

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Контроль и оценка результатов освоения учебной дисциплины осуществляется преподавателем в процессе проведения лабораторных занятий, проверки выполнения самостоятельной работы.

Оценка качества освоения учебной программы включает текущий контроль успеваемости, промежуточную аттестацию по итогам освоения дисциплины.

Результаты обучения: умения, знания компетенции	Форма контроля и оценивания
Уметь:	
-проводить анализ и оценку уязвимостей компьютерной системы;	Тестовые задания, доклады, лабораторные работы, контрольная работа. Зачет
- применять меры информационной безопасности процедурного уровня.	Тестовые задания, доклады, лабораторные работы, контрольная работа. Зачет

- осуществлять защиту информации от несанкционированного доступа.	Тестовые задания, доклады, лабораторные работы, контрольная работа. Зачет
- настраивать безопасность почтового клиента;	Тестовые задания, доклады, лабораторные работы, контрольная работа. Зачет
- настраивать параметры аутентификации пользователей;	Тестовые задания, доклады, лабораторные работы, контрольная работа. Зачет
- осуществлять регистрацию и аудит информационной безопасности;	Тестовые задания, доклады, лабораторные работы, контрольная работа. Зачет
- настраивать системы разграничения доступа;	Тестовые задания, доклады, лабораторные работы, контрольная работа. Зачет
- применять криптографические методы и средства защиты информации;	Тестовые задания, доклады, лабораторные работы, контрольная работа. Зачет
- использовать средства антивирусной защиты;	Тестовые задания, доклады, лабораторные работы, контрольная работа. Зачет
- использовать стандарты и спецификации информационной безопасности;	Тестовые задания, доклады, лабораторные работы, контрольная работа. Зачет
-определять оптимальную конфигурацию оборудования и характеристик устройств для конкретных задач;	Тестовые задания, доклады, лабораторные работы, контрольная работа. Зачет
-идентифицировать основные узлы персонального компьютера, разъемы для подключения внешних устройств;	Тестовые задания, доклады, лабораторные работы, контрольная работа. Зачет
-обеспечивать совместимость аппаратных и программных средств вычислительной техники.	Тестовые задания, доклады, лабораторные работы, контрольная работа. Зачет
Знать	
- понятие и составляющие информационной безопасности;	Тестовые задания, доклады, лабораторные работы, контрольная работа. Зачет
- виды угроз информации и методы защиты от них;	Тестовые задания, доклады, лабораторные работы, контрольная работа. Зачет
- законы, стандарты и спецификации информационной безопасности;	Тестовые задания, доклады, лабораторные работы, контрольная работа. Зачет
- меры процедурного уровня информационной безопасности;	Тестовые задания, доклады, лабораторные работы, контрольная работа. Зачет
- меры программно-технического уровня информационной безопасности;	Тестовые задания, доклады, лабораторные работы, контрольная работа. Зачет
- методы защиты информации от несанкционированного доступа;	Тестовые задания, доклады, лабораторные работы, контрольная работа. Зачет
- способы разграничения полномочий и доступа к объектам;	Тестовые задания, доклады, лабораторные работы, контрольная работа. Зачет
- осуществление регистрации и аудита в компьютерной системе;	Тестовые задания, доклады, лабораторные работы, контрольная работа. Зачет
- проведение оценки рисков компьютерной системы;	Тестовые задания, доклады, лабораторные работы, контрольная работа. Зачет
- применение средств антивирусной защиты.	Тестовые задания, доклады, лабораторные работы, контрольная работа. Зачет
- построение цифровых вычислительных систем и их архитектурные особенности;	Тестовые задания, доклады, лабораторные работы, контрольная работа. Зачет
-принципы работы основных логических блоков системы;	Тестовые задания, доклады, лабораторные работы, контрольная работа. Зачет
-параллелизм и конвейеризацию вычислений;	Тестовые задания, доклады, лабораторные

	работы, контрольная работа. Зачет
-классификацию вычислительных платформ;	Тестовые задания, доклады, лабораторные работы, контрольная работа. Зачет
-принципы вычислений в многопроцессорных и многоядерных системах;	Тестовые задания, доклады, лабораторные работы, контрольная работа. Зачет
-принципы работы кэш-памяти;	Тестовые задания, доклады, лабораторные работы, контрольная работа. Зачет
-методы повышения производительности многопроцессорных и многоядерных систем;	Тестовые задания, доклады, лабораторные работы, контрольная работа. Зачет
-основные энергосберегающие технологии.	Тестовые задания, доклады, лабораторные работы, контрольная работа. Зачет