

Документ подписан простой электронной подписью
 Информация о владельце:
 ФИО: Карпова Елизавета Александровна
 Должность: директор
 Дата подписания: 28.09.2023 13:57:46
 Уникальный программный ключ:
 ad9053b6a9e639199a21a41d1a80dd3f5c40650966caaf85dff11a7fd7d02cbad



СОЦИАЛЬНО-ТЕХНОЛОГИЧЕСКИЙ КОЛЛЕДЖ
 ЧАСТНОЕ УЧРЕЖДЕНИЕ
 ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ

«УТВЕРЖДАЮ»
 Директор ЧУ ПО «СТК»

Е. А. Карпова
 Е. А. Карпова



27.01.2021 г.

Основы информационной безопасности рабочая программа дисциплины (модуля)

Закреплена за кафедрой	Цикловая комиссия по информатике и информационной безопасности		
Учебный план	Направление	10.02.04	Обеспечение информационной безопасности телекоммуникационных систем
Учебный год начала подготовки	2021-2022		
Квалификация	Техник по защите информации		
Форма обучения	очная		
Часов по учебному плану	72	Виды контроля в семестрах:	
в том числе:		зачеты 3	
аудиторные занятия	52		
самостоятельная работа	20		

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	3 (2.1)		Итого	
	Неделя		13	
Вид занятий	уп	рп	уп	рп
Лекции	26	26	26	26
Практические	26	26	26	26
Итого ауд.	52	52	52	52
Контактная работа	52	52	52	52
Сам. работа	20	20	20	20
Итого	72	72	72	72

Рабочая программа дисциплины

Основы информационной безопасности

разработана в соответствии с ФГОС:

Федеральный государственный образовательный стандарт среднего профессионального образования по специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем (приказ Минобрнауки России от 09.12.2016 г. № 1551)

составлена на основании учебного плана:

Направление 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем
утвержденного на заседании Педагогического Совета ЧУ ПО "СТК" 24.01.2022 протокол № 1.

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

1.1	Цель дисциплины: ознакомить студентов с принципами и методами создания, хранения, редактирования, представления и защиты информации, а также с последними достижениями в этих областях, при этом особое внимание акцентируется на изучение специализированного применения технологий обработки информации, необходимого студентам в последующей профессиональной деятельности.
-----	--

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП

Цикл (раздел) ООП:	ОПЦ
2.1	Требования к предварительной подготовке обучающегося:
2.1.1	Вычислительные системы, сети и телекоммуникации
2.1.2	Информационные системы и технологии
2.1.3	Теория вероятностей и математическая статистика
2.1.4	Экономика фирмы (предприятия)
2.1.5	Безопасность жизнедеятельности
2.1.6	Право
2.1.7	История (история России, всеобщая история)
2.1.8	Физическая культура и спорт
2.1.9	Философия
2.2	Дисциплины и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:
2.2.1	Менеджмент
2.2.2	Программная инженерия
2.2.3	Производственная практика (технологическая (проектно-технологическая) практика)
2.2.4	Подготовка к сдаче и сдача государственного экзамена
2.2.5	Выполнение работ по одной или нескольким профессиям рабочих, должностям служащих (для специальностей СПО)
2.2.6	Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных (в том числе, криптографических) средств защиты
2.2.7	Защита информации в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

ОК 01.: Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.

Знать:	
1	содержание основных понятий обеспечения информационной безопасности
2	источники угроз безопасности информации;
3	методы оценки уязвимости информации
Уметь:	
1	находить необходимые нормативные правовые акты и информационные правовые нормы в системе действующего законодательства, в том числе с помощью систем правовой информации;
2	применять действующую законодательную базу в области информационной безопасности;
3	разрабатывать проекты положений, инструкций и других организационно-распорядительных документов, регламентирующих работу по защите информации.
Владеть:	
1	об основных понятиях теории информации
2	о методах и средствах обеспечения информационной безопасности;
3	о методах нарушения конфиденциальности целостности и доступности информации

ОК 02.: Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.

Знать:	
1	находить необходимые нормативные правовые акты и информационные правовые нормы в системе действующего законодательства, в том числе с помощью систем правовой информации
2	применять действующую законодательную базу в области информационной безопасности;

3	разрабатывать проекты положений, инструкций и других организационно-распорядительных документов, регламентирующих работу по защите информации.
Уметь:	
1	Обрабатывать статический информационный контент.
2	Осуществлять сбор и анализ информации для определения потребностей клиента.
3	Проводить адаптацию отраслевого программного обеспечения
Владеть:	
1	Понимать сущность и социальную значимость своей будущей профессии, проявлять к ней устойчивый интерес
2	Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество;
3	Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность;

ОК 03.: Планировать и реализовывать собственное профессиональное и личностное развитие.

Знать:	
1	Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития
2	Использовать информационно-коммуникационные технологии в профессиональной деятельности
3	Работать в коллективе и в команде, эффективно общаться с коллегами, руководством, потребителями
Уметь:	
1	Брать на себя ответственность за работу членов команды (починенных), за результат выполнения заданий;
2	Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации;
3	Ориентироваться в условиях частой смены технологий в профессиональной деятельности.
Владеть:	
1	Исполнять воинскую обязанность, в том числе с применением полученных профессиональных знаний (для юношей)
2	Понимать сущность и социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности
3	организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество

ОК 04.: Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.

Знать:	
1	организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество
2	принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность
3	принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность
Уметь:	
1	номенклатура информационных источников применяемых в профессиональной деятельности; приемы структурирования информации; формат оформления результатов поиска информации
2	осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития.
3	Использовать информационно-коммуникационные технологии в профессиональной деятельности
Владеть:	
1	самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации
2	ориентироваться в условиях частой смены технологий в профессиональной деятельности
3	ориентироваться в условиях частой смены технологий в профессиональной деятельности

ОК 05.: Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.

Знать:	
1	Использовать информационно-коммуникационные технологии в профессиональной деятельности;
2	Работать в коллективе и в команде, эффективно общаться с коллегами, руководством, потребителями;
3	Брать на себя ответственность за работу членов команды (починенных), за результат выполнения заданий;
Уметь:	

1	Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации;
2	Ориентироваться в условиях частой смены технологий в профессиональной деятельности.
3	Исполнять воинскую обязанность, в том числе с применением полученных профессиональных знаний (для юношей)

Владеть:

1	Понимать сущность и социальную значимость своей будущей профессии, проявлять к ней устойчивый интерес;
2	Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество;
3	Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность

ОК 09.: Использовать информационные технологии в профессиональной деятельности.**Знать:**

1	содержание основных понятий обеспечения информационной безопасности;
2	источники угроз безопасности информации
3	методы оценки уязвимости информации

Уметь:

1	находить необходимые нормативные правовые акты и информационные правовые нормы в системе действующего законодательства, в том числе с помощью систем правовой информации;
2	применять действующую законодательную базу в области информационной безопасности;
3	разрабатывать проекты положений, инструкций и других организационно-распорядительных документов, регламентирующих работу по защите информации.

Владеть:

1	об основных понятиях теории информации
2	о методах и средствах обеспечения информационной безопасности
3	о методах нарушения конфиденциальности целостности и доступности информации;

ОК 10.: Пользоваться профессиональной документацией на государственном и иностранном языке.**Знать:**

1	содержание основных понятий обеспечения информационной безопасности;
2	источники угроз безопасности информации;
3	методы оценки уязвимости информации;

Уметь:

1	находить необходимые нормативные правовые акты и информационные правовые нормы в системе действующего законодательства, в том числе с помощью систем правовой информации;
2	применять действующую законодательную базу в области информационной безопасности
3	разрабатывать проекты положений, инструкций и других организационно-распорядительных документов, регламентирующих работу по защите информации.

Владеть:

1	Обрабатывать статический информационный контент
2	Обрабатывать динамический информационный контент
3	Осуществлять сбор и анализ информации для определения потребностей клиента

ПК 1.2.: Осуществлять диагностику технического состояния, поиск неисправностей и ремонт оборудования информационно-телекоммуникационных систем и сетей.**Знать:**

1	Понимать сущность и социальную значимость своей будущей профессии, проявлять к ней устойчивый интерес;
2	Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество;
3	Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность

Уметь:

1	Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития;
2	Использовать информационно-коммуникационные технологии в профессиональной деятельности;
3	Работать в коллективе и в команде, эффективно общаться с коллегами, руководством, потребителями;

Владеть:

1	Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество;
2	Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность;
3	Использовать информационно-коммуникационные технологии в профессиональной деятельности

ПК 1.4.: Осуществлять контроль функционирования информационно-телекоммуникационных систем и сетей.

Знать:	
1	содержание основных понятий обеспечения информационной безопасности
2	источники угроз безопасности информации
3	методы оценки уязвимости информации
Уметь:	
1	находить необходимые нормативные правовые акты и информационные правовые нормы в системе действующего законодательства, в том числе с помощью систем правовой информации
2	применять действующую законодательную базу в области информационной безопасности;
3	разрабатывать проекты положений, инструкций и других организационно-распорядительных документов, регламентирующих работу по защите информации
Владеть:	
1	Обеспечивать технику безопасности при проведении организационно-технических мероприятий
2	Применять программно-аппаратные и технические средства защиты информации на объектах профессиональной деятельности.
3	участвовать в эксплуатации систем и средств защиты информации защищаемых объектов

В результате освоения дисциплины обучающийся должен

3.1	Знать:
3.1.1	Основы теории информационной безопасности, классификацию и основное содержание нормативных документов в данной области.
3.2	Уметь:
3.2.1	Использовать полученные навыки по реализации технологий, направленных на обеспечение информационной безопасности в условиях операционной системы Windows, ее приложений, локальных и общемировых сетей.
3.3	Владеть:
3.3.1	Опытом (навыком) работы с антивирусными пакетами, настройки параметров информационной безопасности в приложениях – браузерах сети Internet.

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов
	Раздел 1. ИБ как потребность в условиях информатизации современного общества. Основы теории информационной безопасности. Угрозы и нарушители ИБ. Стандарты ИБ. Характеристики безопасности для различных информационных объектов.		
1.1	Информационная безопасность и ее аспекты. /Лек/	3	5
1.2	Общие положения теории информационной безопасности. /Лек/	3	4
1.3	Стратегии защиты информации. /Лек/	3	6
1.4	Угрозы информационной безопасности. /Лек/	3	5
1.5	Методы криптографии. /Пр/	3	5
1.6	Центр обеспечения безопасности Windows. /Пр/	3	4
1.7	Локальная политика безопасности при администрировании Windows. /Пр/	3	5
1.8	Информационная безопасность и ее аспекты. /Ср/	3	1
1.9	Общие положения теории информационной безопасности. /Ср/	3	1
1.10	Стратегии защиты информации. /Ср/	3	1
1.11	Нарушители и нарушения информационной безопасности. /Ср/	3	1
1.12	Защита информационной безопасности. /Ср/	3	1
1.13	Угрозы информационной безопасности. /Ср/	3	1
1.14	Стандарты и спецификации в области информационной безопасности. /Лек/	3	2
1.15	Административный уровень информационной безопасности /Лек/	3	2
1.16	Общие сведения о стандартах и спецификациях в области информационной безопасности. /Лек/	3	1

1.17	Безопасность локальных объектов и локальных сетей. /Лек/	3	1
1.18	Информационная безопасность в условиях локальных сетей. /Пр/	3	4
1.19	Сеансовое конфигурирование Windows. /Пр/	3	4
1.20	Информационная безопасность в СУБД Access. /Пр/	3	4
1.21	Стандарты и спецификации в области информационной безопасности. /Ср/	3	2
1.22	Административный уровень информационной безопасности. /Ср/	3	2
1.23	Общие сведения о стандартах и спецификациях в области информационной безопасности. /Ср/	3	2
1.24	Безопасность локальных объектов и локальных сетей. /Ср/	3	2
1.25	Обеспечение информационной безопасности в общемировых сетях. /Ср/	3	2
1.26	/Зачёт/	3	4

5. ОЦЕНОЧНЫЕ СРЕДСТВА

5.1. Вопросы для самоконтроля и текущей аттестации

Понятие информационной безопасности.
 Концепция информационной безопасности.
 Место информационной безопасности экономических систем в национальной безопасности страны.
 Важность и сложность проблемы информационной безопасности.
 Информационная безопасность в условиях функционирования в России глобальных сетей.
 Теория информационной безопасности информационных систем, ее основные составляющие и задачи.
 Моделирование процессов защиты информации.
 Модели безопасности и их применение.
 Понятие стратегии защиты. Виды стратегий защиты.
 Критерии обоснования стратегии защиты.
 Понятие угрозы безопасности информации и общие подходы к ее классификации.
 Классификация угроз безопасности информации по способам их возможного негативного воздействия.
 Угрозы доступности, целостности, конфиденциальности.
 Происхождение угроз безопасности информации.
 Предпосылки появления угроз.
 Понятие нарушителя безопасности информации.
 Виды противников или нарушителей безопасности информации.
 Виды возможных нарушений информационной системы.
 Таксономия нарушений информационной безопасности вычислительной системы и причины, обуславливающие их существование.
 Анализ способов нарушений информационной безопасности.
 Вирус как типичное нарушение информационной безопасности. Виды вирусов.
 Понятие системы защиты информации.
 Типизация и стандартизация систем защиты информации.
 Центры защиты информации и их функции.
 Основные технологии построения защищенных ЭИС.
 Использование защищенных ЭИС.
 Понятие криптографии. Методы криптографии.
 Политика безопасности.
 Программа безопасности.
 Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы.
 Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства.
 Международные стандарты информационного обмена.
 Стандарты и спецификации в области информационной безопасности и их классификация.
 «Оранжевая книга».
 Гармонизированные критерии европейских стран.
 Спецификация internet-сообщества RFC 1510 «сетевой сервис аутентификации kerberos (v5)».
 Руководящие документы (РД) Гостехкомиссии России.
 X.800 «архитектура безопасности для взаимодействия открытых систем».
 Технические спецификации IPSEC, TLS.
 Рекомендация «как выбирать поставщика internet-услуг».
 Британский стандарт BS 7799 «управление информационной безопасностью. Практические правила».
 Безопасность операционных систем.
 Безопасность систем управления базами данных.
 Безопасность виртуальных частных сетей.
 Безопасность виртуальных локальных сетей.
 Безопасность смарт – карт.
 Архитектура средств безопасности IP-уровня.
 Контексты безопасности и управление ключами.

Обеспечение аутентичности IP-пакетов. Обеспечение конфиденциальности сетевого трафика. Роль поставщика internet-услуг в реагировании на нарушения безопасности. Меры по защите internet-сообщества. Обеспечение безопасности маршрутизаторов. Особенности использования управляющих протоколов. Безопасное размещение сетевого оборудования потребителя. Защита системной инфраструктуры.
5.2. Темы письменных работ (контрольных и курсовых работ, рефератов)
Учебным планом не предусмотрены.
5.3. Оценочные средства для промежуточной аттестации
ФОС представлен в УМК дисциплины.

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)			
6.1. Рекомендуемая литература			
6.1.1. Основная литература			
	Авторы, составители	Заглавие	Издательство, год, эл. адрес
Л1.1	Артемов А. В.	Информационная безопасность: курс лекций: Учебная литература для ВУЗов	Орел: МАБИВ, 2014 http://biblioclub.ru/index.php?page=book&id=428605&sr=1
Л1.2	Башлы П. Н. , Баранова Е. К. , Бабаш А. В.	Информационная безопасность: Учебно-практическое пособие	М.: Евразийский открытый институт, 2011 http://biblioclub.ru/index.php?page=book_red&id=90539
6.1.2. Дополнительная литература			
	Авторы, составители	Заглавие	Издательство, год, эл. адрес
Л2.1	Колябин А.Ю.	Информационная безопасность и защита информации: сборник студенческих работ	Москва: Студенческая наука,, 2012 https://biblioclub.ru/index.php?page=book_red&id=227774&sr=1
6.2.1 Перечень программного обеспечения			
6.3.1.1	Microsoft Windows, OpenOffice, доступ в сеть Интернет.		
6.2.2 Перечень информационных справочных систем и ресурсов сети Интернет			
6.3.2.1	Каталог документов по направлению Информационная безопасность https://cisoclub.ru/doc/		
6.3.2.2	Журнал «Информационная безопасность» https://www.itsec.ru/		

7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)	
7.1	Специальные помещения представляют собой учебные аудитории для проведения занятий лекционного типа, занятий семинарского типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, а также помещения для самостоятельной работы и помещения для хранения и профилактического обслуживания учебного оборудования. Специальные помещения укомплектованы специализированной мебелью и техническими средствами обучения, служащими для представления учебной информации большой аудитории. Для проведения занятий лекционного типа предлагаются наборы демонстрационного оборудования и учебно-наглядных пособий, обеспечивающие тематические иллюстрации, соответствующие примерным программам дисциплин (модулей), рабочим учебным программам дисциплин (модулей). Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно - образовательную среду.

8. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)	
Обучающимся необходимо помнить, что качество полученного образования в немалой степени зависит от активной роли самого обучающегося в учебном процессе. Обучающийся должен быть нацелен на максимальное усвоение подаваемого лектором материала, после лекции и во время специально организуемых индивидуальных встреч он может задать лектору интересующие его вопросы. Лекционные занятия составляют основу теоретического обучения и должны давать систематизированные основы знаний по дисциплине, раскрывать состояние и перспективы развития соответствующей области науки, концентрировать внимание обучающихся на наиболее сложных и узловых вопросах, стимулировать их активную познавательную деятельность и способствовать формированию творческого мышления.	

Главная задача лекционного курса - сформировать у обучающихся системное представление об изучаемом предмете, обеспечить усвоение будущими специалистами основополагающего учебного материала, принципов и закономерностей развития соответствующей научно-практической области, а также методов применения полученных знаний, умений и навыков.

Основные функции лекций: 1. Познавательная-обучающая; 2. Развивающая; 3. Ориентирующе-направляющая; 4. Активизирующая; 5. Воспитательная; 6. Организующая; 7. информационная.

Выполнение практических заданий служит важным связующим звеном между теоретическим освоением данной дисциплины и применением ее положений на практике. Они способствуют развитию самостоятельности обучающихся, более активному освоению учебного материала, являются важной предпосылкой формирования профессиональных качеств будущих специалистов.

Проведение практических занятий не сводится только к органическому дополнению лекционных курсов и самостоятельной работы обучающихся. Их вместе с тем следует рассматривать как важное средство проверки усвоения обучающимися тех или иных положений, даваемых на лекции, а также рекомендуемой для изучения литературы; как форма текущего контроля за отношением обучающихся к учебе, за уровнем их знаний, а следовательно, и как один из важных каналов для своевременного подтягивания отстающих обучающихся.

При подготовке важны не только серьезная теоретическая подготовка, но и умение ориентироваться в разнообразных практических ситуациях, ежедневно возникающих в его деятельности. Этому способствует форма обучения в виде практических занятий. Задачи практических занятий: закрепление и углубление знаний, полученных на лекциях и приобретенных в процессе самостоятельной работы с учебной литературой, формирование у обучающихся умений и навыков работы с исходными данными, научной литературой и специальными документами. Практическому занятию должно предшествовать ознакомление с лекцией на соответствующую тему и литературой, указанной в плане этих занятий.

При проведении учебных занятий обеспечиваются развитие у обучающихся навыков командной работы, межличностной коммуникации, принятия решений, лидерских качеств (включая при необходимости проведение интерактивных лекций, групповых дискуссий, ролевых игр, тренингов, анализ ситуаций и имитационных моделей, преподавание дисциплин (модулей) в форме курсов, составленных на основе результатов научных исследований, проводимых организацией, в том числе с учетом региональных особенностей профессиональной деятельности выпускников и потребностей работодателей). Самостоятельная работа может быть успешной при определенных условиях, которые необходимо организовать. Ее правильная организация, включающая технологии отбора целей, содержания, конструирования заданий и организацию контроля, систематичность самостоятельных учебных занятий, целесообразное планирование рабочего времени позволяет привить студентам умения и навыки в овладении, изучении, усвоении и систематизации приобретаемых знаний в процессе обучения, привить навыки повышения профессионального уровня в течение всей трудовой деятельности.

Для контроля знаний студентов по данной дисциплине необходимо проводить оперативный, рубежный и итоговый контроль.

Оперативный контроль осуществляется путем проведения опросов студентов на семинарских занятиях, проверки выполнения практических заданий, а также учета вовлеченности (активности) студентов при обсуждении мини-докладов, организации ролевых игр и т.п.

Контроль за самостоятельной работой студентов по курсу осуществляется в двух формах: текущий контроль и итоговый. Рубежный контроль (аттестация) подразумевает проведение тестирования по пройденным разделам курса. В тестирование могут быть включены темы, предложенные студентам для самостоятельной подготовки, а также практические задания.