

УТВЕРЖДАЮ  
Директор ВШТЭ

## РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

<b>Б1.В.01</b> <small>(индекс дисциплины)</small>	<b>Защита информации в системах управления и автоматизации</b> <small>(Наименование дисциплины)</small>
Кафедра: <b>1</b> <small>Код</small>	Информационно-измерительных технологий и систем управления <small>(Наименование кафедры)</small>
Направление подготовки:	27.03.04 Управление в технических системах
Профиль подготовки:	Системы и средства автоматизации технологических процессов
Уровень образования :	бакалавриат

### План учебного процесса

Составляющие учебного процесса		Очное обучение	Очно-заочное обучение	Заочное обучение
Контактная работа обучающихся с преподавателем по видам учебных занятий и самостоятельная работа обучающихся (часы)	Всего	<b>144</b>		
	Аудиторные занятия	<b>54</b>		
	Лекции	18		
	Лабораторные занятия			
	Практические занятия	36		
	Самостоятельная работа	<b>90</b>		
	Промежуточная аттестация			
Формы контроля по семестрам (номер семестра)	Экзамен			
	Зачет	3		
	Курсовой проект (работа)			
<b>Общая трудоемкость дисциплины (зачетные единицы)</b>		<b>4</b>		

Форма обучения:	Распределение зачетных единиц трудоемкости по семестрам									
	1	2	3	4	5	6	7	8	9	10
Очная			<b>4</b>							
Очно-заочная										
Заочная										

Рабочая программа дисциплины составлена в соответствии с федеральным  
государственным образовательным стандартом высшего образования  
по направлению подготовки 27.03.04 Управление в технических системах

На основании учебного плана № b270304-123\_20

Кафедра-разработчик: информационно-измерительных технологий и систем управления

Заведующий кафедрой: Сидельников В.И.

### **СОГЛАСОВАНИЕ:**

Выпускающая кафедра: информационно-измерительных технологий и систем управления

Заведующий кафедрой: Сидельников В.И.

Методический отдел: Смирнова В.Г.

# 1. ВВЕДЕНИЕ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ

## 1.1. Место преподаваемой дисциплины в структуре образовательной программы

Блок 1: Базовая  Обязательная  Дополнительно является факультативом   
Вариативная  По выбору

## 1.2. Цель дисциплины

Целью дисциплины является формирование у студентов знаний в области теоретических основ информационной безопасности, ознакомление студентов с тенденцией развития информационной безопасности, с моделями возможных угроз и основными нормативными документами России, по данному вопросу, формирование практических умений и навыков применения современных технологий обеспечения защиты информации.

## 1.3. Задачи дисциплины

- Рассмотреть существующие угрозы безопасности информации;
- Раскрыть принципы и методы подбора и применения современных методов и способов защиты информации;
- Приобрести практические навыки работы по защите информации.

## 1.4. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

Код компетенции	Формулировка компетенции	Этап формирования
ОПК- 6	способностью осуществлять поиск, хранение, обработку и анализ информации из различных источников и баз данных, представлять ее в требуемом формате с использованием информационных, компьютерных и сетевых технологий	2
Планируемые результаты обучения Знать: 1) Основные методы использования современных программных средств для обеспечения информационной безопасности; 2) Механизмы возникновения нарушений информационной безопасности. Уметь: 1) Использовать методы защиты информационных систем; 2) Ориентироваться в нестандартных ситуациях, нести социальную и этическую ответственность за принятые решения. Владеть: 1) Терминологией в области защиты информационной безопасности; 2) Навыками работы по защите компьютерной информации.		
ПК- 3	готовностью участвовать в составлении аналитических обзоров и научно-технических отчетов по результатам выполненной работы, в подготовке публикаций по результатам исследований и разработок	2
Планируемые результаты обучения Знать: 1) основные требования к составлению аналитических обзоров и научно-технических отчетов 2) способы представления результатов исследований и разработок и подготовки публикаций Уметь: 1) составлять аналитические обзоры и научно – технические отчеты по результатам исследований и выполняемым работам 2) представлять результаты выполняемых работ и готовить публикации по результатам исследований Владеть: 1) навыками составления аналитических обзоров и подготовке публикаций по результатам исследований разработок методами представления результатов исследования и разработок и выполненных работ в виде отчетов и публикаций		

**1.5. Дисциплины (практики) образовательной программы, в которых было начато формирование компетенций, указанных в п.1.4:**

- Информатика (ОПК-6)

**2. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ**

Наименование и содержание учебных модулей, тем и форм контроля	Объем (часы)		
	очное обучение	очно-заочное обучение	заочное обучение
<b>Учебный модуль 1. Основы информационной безопасности</b>			
Тема 1. Теоретические основы информационной безопасности Современное состояние защиты информации. Понятие, основные определения и составляющие информационной безопасности. Доступность, целостность, конфиденциальность.	10		
Тема 2. Актуальность защиты информации Важность и сложность проблемы информационной безопасности. Анализ проблематики, связанной с информационной безопасностью. Проблемы защиты информации в интернете. Ценность информации.	10		
<b>Текущий контроль 1. Опрос</b>	2		
<b>Учебный модуль 2. Угрозы информационной безопасности</b>			
Тема 3. Виды угроз Наиболее распространенные угрозы, пути и каналы утечки информации, от кого они исходят и к чему приводят. Изучение видов атак и методов взлома интрасетей злоумышленниками. Виды возможных нарушений информационной системы. Виды противников или «нарушителей».	14		
Тема 4. Вредоносное программное обеспечение. Основные правила защиты от «компьютерных вирусов». Обзор и методика использования антивирусных программ. Восстановление пораженных «компьютерными вирусами» объектов.	14		
<b>Текущий контроль 2. Опрос</b>	2		
<b>Учебный модуль 3. Законодательство в области информационной безопасности</b>			
Тема 5. Основы законодательства в области информационной безопасности Что такое законодательный уровень информационной безопасности и почему он важен. Обзор российского законодательства в области ИБ. Обзор зарубежного законодательства в области ИБ. Критерии безопасности компьютерных систем. Стандарт США «Оранжевая книга».	12		
Тема 6. Лицензирование и сертификация в информационной безопасности Нормы и требования российского законодательства в области лицензирования и сертификации. Порядок оформления и получения лицензий и сертификатов в области ИБ. Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы.	16		
<b>Текущий контроль 3. Опрос</b>	2		
<b>Учебный модуль 4. Программно-технические меры обеспечения компьютерной безопасности информационных систем</b>			
Тема 7. Технические средства защиты информации Способы и средства защиты информации от утечки по техническим каналам. Методы и средства контроля эффективности защиты объектов информатизации, и от утечки информации по техническим каналам.	20		
Тема 8. Программно-технические меры защиты информации Основные понятия программно-технического уровня информационной безопасности. Рассматриваются методы защиты информации: ограничение доступа, разграничение доступа, разделение доступа, криптографическое преобразование информации, контроль и учет доступа, законодательные меры, обеспечение информационной безопасности в Internet. Основные технологии построения защищенных ИС.	30		
<b>Текущий контроль 4. Опрос</b>	2		
<b>Промежуточная аттестация по дисциплине – Зачет</b>	10		
<b>ВСЕГО:</b>	<b>144</b>		

### 3. ТЕМАТИЧЕСКИЙ ПЛАН

#### 3.1. Лекции

Номера изучаемых тем	Очное обучение		Очно-заочное обучение		Заочное обучение	
	Номер семестра	Объем (часы)	Номер семестра	Объем (часы)	Номер семестра	Объем (часы)
1.	3	1				
2.	3	1				
3.	3	2				
4.	3	2				
5.	3	2				
6.	3	3				
7.	3	3				
8.	3	4				
<b>ВСЕГО:</b>		<b>18</b>				

#### 3.2. Практические занятия

Номера изучаемых тем	Наименование и форма занятий	Очное обучение		Очно-заочное обучение		Заочное обучение	
		Номер семестра	Объем (часы)	Номер семестра	Объем (часы)	Номер семестра	Объем (часы)
1.	Основные составляющие информационной безопасности	3	2				
2.	Анализ проблематики, связанной с информационной безопасностью	3	2				
3.	Изучение видов атак и методов взлома интрасетей злоумышленниками	3	4				
4.	Восстановление пораженных «компьютерными вирусами» объектов	3	4				
5.	Обзор российского и зарубежного законодательства в области информационной безопасности	3	4				
6.	Порядок оформления и получения лицензий и сертификатов в области ИБ	3	4				
7.	Методы и средства защиты информации от утечки по техническим каналам	3	8				
8.	Программные методы защиты информации	3	8				
<b>ВСЕГО:</b>		<b>36</b>					

#### 3.3. Лабораторные занятия

Не предусмотрено.

### 4. КУРСОВОЕ ПРОЕКТИРОВАНИЕ

Не предусмотрено.

### 5. ТЕКУЩИЙ КОНТРОЛЬ УСПЕВАЕМОСТИ ОБУЧАЮЩЕГОСЯ

Номера учебных модулей, по которым проводится контроль	Форма контроля знаний	Очное обучение		Очно-заочное обучение		Заочное обучение	
		Номер семестра	Кол-во	Номер семестра	Кол-во	Номер семестра	Кол-во

Номера учебных модулей, по которым проводится контроль	Форма контроля знаний	Очное обучение		Очно-заочное обучение		Заочное обучение	
		Номер семестра	Кол-во	Номер семестра	Кол-во	Номер семестра	Кол-во
1, 2, 3, 4	Опрос	3	4				

## 6. САМОСТОЯТЕЛЬНАЯ РАБОТА ОБУЧАЮЩЕГОСЯ

Виды самостоятельной работы обучающегося	Очное обучение		Очно-заочное обучение		Заочное обучение	
	Номер семестра	Объем (часы)	Номер семестра	Объем (часы)	Номер семестра	Объем (часы)
Усвоение теоретического материала	3	40				
Подготовка к практическим занятиям	3	40				
Подготовка к зачету	3	10				
<b>ВСЕГО:</b>		<b>90</b>				

## 7. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

### 7.1. Характеристика видов и используемых инновационных форм учебных занятий

Не предусмотрено.

### 7.2. Система оценивания успеваемости и достижений обучающихся для промежуточной аттестации

традиционная

балльно-рейтинговая

## 8. ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

### 8.1. Учебная литература

#### а) основная учебная литература

1. Галас В.П. Автоматизация проектирования систем и средств управления [Электронный ресурс]: учебник/ Галас В.П.— Электрон. текстовые данные.— Владимир: Владимирский государственный университет им. А.Г. и Н.Г. Столетовых, 2015.— 255 с.— (Режим доступа: <http://www.iprbookshop.ru/57362>) - ЭБС «IPRbooks».

2. Метелица Н.Т. Вычислительные сети и защита информации [Электронный ресурс]: учебное пособие/ Метелица Н.Т.— Электрон. текстовые данные.— Краснодар: Южный институт менеджмента, 2013.— 48 с.— (Режим доступа: <http://www.iprbookshop.ru/25962>) - ЭБС «IPRbooks».

#### б) дополнительная учебная литература

3. Иншаков М.В. Технологии и средства реализации информационных процессов в вычислительных сетях [Электронный ресурс]: учебное пособие/ Иншаков М.В.— Электрон. текстовые данные.— М.: Московский городской педагогический университет, 2013.— 164 с.— (Режим доступа: <http://www.iprbookshop.ru/26632>) - ЭБС «IPRbooks».

4. Основы информационных технологий [Электронный ресурс]/ С.В. Назаров [и др.].— Электрон. текстовые данные.— М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.— 530 с.— (Режим доступа: <http://www.iprbookshop.ru/52159>) - ЭБС «IPRbooks».

### 8.2. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

Не предусмотрено.

### 8.3. Перечень ресурсов информационно-телекоммуникационной сети "Интернет", необходимых для освоения дисциплины

1. Защита информации. Необходимая информативная база [Электронный ресурс]. URL: <http://www.mirash.ru/doki11.html>.

2. Защита информации в компьютерных системах [Электронный ресурс]. URL: <http://www.hackzona.ru/hz.php?file=article&name=News&sid=40>.

3. Разработка системы технической защиты средств обработки хранения и передачи информации [Электронный ресурс]. URL: <http://reftrend.ru/462976.html>.

#### 8.4. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем

1. Microsoft Windows 8.1.
2. Microsoft Office Professional 2013.

#### 8.5. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

1. Стандартно оборудованная аудитория.
2. Видеопроектор с экраном.

#### 8.6. Иные материалы

Презентация на тему «Обзор и использование антивирусных программ».

Презентация на тему «Криптографическое преобразование информации».

### 9. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Виды учебных занятий и самостоятельная работа обучающихся	Организация деятельности обучающегося
Лекции	<p>На лекциях обеспечивается теоретическое изучение дисциплины, излагается основное содержание курса, иллюстрируемое конкретными примерами, используется зарубежный и отечественный опыт по защите информации.</p> <p>Освоение лекционного материала обучающимся предполагает следующие виды работ:</p> <ul style="list-style-type: none"> <li>• проработка рабочей программы в соответствии с целями и задачами, структурой и содержанием дисциплины;</li> <li>• конспект лекций: кратко, схематично, последовательно фиксировать основные положения и выводы; помечать важные мысли, выделять ключевые слова, термины.</li> <li>• проверка терминов, понятий: осуществлять с помощью энциклопедий, словарей, справочников с выписыванием толкований в тетрадь;</li> <li>• при конспектировании источников: найти ответ на вопросы в рекомендуемой литературе.</li> </ul> <p>Если самостоятельно не удастся разобраться в материале, необходимо сформулировать вопрос и задать преподавателю на консультации или на практическом занятии.</p>
Практические занятия	<p>На практических занятиях разъясняются теоретические положения курса, обучающиеся работают с конкретными ситуациями, овладевают навыками сбора, анализа и обработки информации для принятия самостоятельных решений, навыками подготовки информационных обзоров и аналитических отчетов по соответствующей тематике; навыками работы в малых группах.</p> <p>Подготовка к практическим занятиям предполагает следующие виды работ:</p> <ul style="list-style-type: none"> <li>• подготовка ответов к контрольным вопросам;</li> <li>• работа с текстами из списка рекомендуемой основной и дополнительной литературы.</li> </ul>
Самостоятельная работа	<p>Самостоятельная работа студента предполагает расширение и закрепление знаний, умений и навыков, усвоенных на аудиторных занятиях путем самостоятельной проработки учебно-методических материалов по дисциплине и другим источникам информации, а также подготовки к зачету.</p> <p>Самостоятельная работа выполняется индивидуально, а также может проводиться под руководством (при участии) преподавателя. Следует предварительно изучить методические указания по выполнению самостоятельной работы.</p> <p>При подготовке к зачету необходимо ознакомиться с перечнем вопросов, проработать конспекты практических занятий, рекомендуемую литературу, получить консультацию у преподавателя, подготовить презентацию</p>

Виды учебных занятий и самостоятельная работа обучающихся	Организация деятельности обучающегося
	материалов.

## 10. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

### 10.1. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

#### 10.1.1. Показатели оценивания компетенций на этапах их формирования

Код компетенции (этап освоения)	Показатели оценивания компетенций	Наименование оценочного средства	Представление оценочного средства в фонде
ОПК-6 (2)	1. Обладает навыками поиска, хранения и обработки информации из различных источников и баз данных 2. Использует современные методы защиты информационных систем для обеспечения информационной безопасности 3. Демонстрирует навыки пользования современными программными средствами для обеспечения защиты информации	1. Устное собеседование 2. Тестовое задание 3. Практическое типовое задание	1. Перечень вопросов зачету (40 вопросов) 2. Тестовые задания по вариантам (3 варианта по 40 заданий в каждом) 3. Типовые задачи по вариантам (5 вариантов по 2 задачи в каждом)
ПК-3(2)	1. Демонстрирует основные требования к составлению отчетов аналитических обзоров по результатам выполненных работ и исследований. 2. Показывает как составлять аналитические обзоры и научно-технические отчеты по результатам. 3. Использует навыками составления аналитических обзоров и подготовке публикаций по результатам исследований разработок.	1. Устное собеседование 2. Тестовое задание 3. Практическое типовое задание	1. Перечень вопросов зачету (40 вопросов) 2. Тестовые задания по вариантам (3 варианта по 40 заданий в каждом) 3. Типовые задачи по вариантам (5 вариантов по 2 задачи в каждом)

#### 10.1.2. Описание шкал и критериев оценивания сформированности компетенций

##### Критерии оценивания сформированности компетенций

Оценка по традиционной шкале	Критерии оценивания сформированности компетенций
Зачтено	Обучающийся своевременно выполнил тестовое задание, решил типовые задачи, свободно ориентируется в основных понятиях и терминах по защите информации; усвоил основную и знаком с дополнительной литературой по обеспечению информационной безопасности, возможно допустил несущественные ошибки в ответе на вопросы преподавателя
Не зачтено	Обучающийся не выполнил тестовое задание, не решил типовые задачи, не способен сформулировать хотя бы отдельные концепции по защите



Оценка по традиционной шкале	Критерии оценивания сформированности компетенций
	информации, допустил существенные ошибки в ответе на вопросы преподавателя. Попытка списывания, использования неразрешенных технических устройств или пользование подсказкой другого человека.

**10.2. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующие этапы формирования компетенций**

**10.2.1. Перечень вопросов к зачету, разработанный в соответствии с установленными этапами формирования компетенций**

№ п/п	Формулировка вопросов	№ темы
1	Сформулируйте понятия и основные составляющие информационной безопасности	1
2	Определите понятия «безопасность информации» и его отличие от понятия «защита информации»	1
3	Назовите объекты защиты при обеспечении компьютерной безопасности	1
4	Какие Вы знаете категории и носители информации	1
5	Сформулируйте понятия «доступность», «целостность», «конфиденциальность информации»	1
6	Обоснуйте важность проблемы компьютерной информационной безопасности	2
7	Классификация информации по степени важности	2
8	Обоснуйте проблемы защиты информации в интернете	2
9	Сформулируйте понятие «ценность информации». Назовите порядковую шкалу ценностей	2
10	Формулировка актуальности решения проблем защиты информации	2
11	Назовите наиболее распространенные угрозы для компьютерной информации	3
12	Назовите наиболее распространенные пути и каналы утечки информации	3
13	Назовите виды атак и методы взлома информационных сетей злоумышленниками	3
14	Сформулируйте виды противников или «нарушителей» информационной безопасности	3
15	Назовите виды возможных нарушений информационной системы	3
16	Сформулируйте понятие «Вредоносные программы (вирусы)». Классификация компьютерных вирусов	4
17	Назовите основные правила защиты от компьютерных вирусов	4
18	Назовите современные антивирусные программы	4
19	Сформулируйте достоинства и недостатки современных антивирусных программ	4
20	Назовите признаки заражения компьютера от вредоносных программ	4
21	Сформулируйте понятие законодательного уровня информационной безопасности	5
22	Объясните важность законодательного уровня информационной безопасности	5
23	Назовите критерии безопасности компьютерных систем	5
24	Сформулируйте текущее состояние российского законодательства в области информационной безопасности	5
25	В каком случае сотрудник учреждения может быть привлечен к ответственности за нарушения правил информационной безопасности?	5
26	Назовите требования российского законодательства в области лицензирования и сертификации	6
27	Сформулируйте основные понятия в области лицензирования	
28	Объясните порядок оформления и получения лицензий в области информационной безопасности	6
29	Сформулируйте причины отказа в получении лицензии	6
30	Объясните порядок оформления и получения сертификатов в области информационной безопасности	6
31	Сформулируйте понятие «утечка данных». Назовите каналы утечки и нарушения безопасности компьютерной информации	7

№ п/п	Формулировка вопросов	№ темы
32	Назовите способы защиты информации от утечки по техническим каналам	7
33	Какие вы знаете современные технические средства защиты информации	7
34	Классификация технических средств защиты информации	7
35	Назовите мероприятия по защите информации от несанкционированного доступа	7
36	Назовите методы защиты информации	8
37	Сформулируйте понятие «Идентификация пользователей». Классификация методов идентификации пользователей	8
38	Сформулируйте понятия и дайте характеристику «аутентификация пользователей», «парольная аутентификация»	8
39	Дайте определение понятиям «Управление доступом, ограничение, разграничение, разделение доступа к информации» и сформулируйте их основные характеристики	8
40	Сформулируйте преимущества и недостатки метода криптографического преобразования информации	8

**Вариант тестовых заданий, разработанных в соответствии с установленными этапами формирования компетенций**

№ п/п	Формулировка задания	Ответ
1	<b>Тема 1. Теоретические основы информационной безопасности</b> Защита информации это: а) деятельность по предотвращению утечки информации, несанкционированных и непреднамеренных воздействий на неё б) процесс сбора, накопления, обработки, хранения, распределения и поиска информации в) преобразование информации, в результате которого содержание информации становится непонятным для субъекта, не имеющего доступа	а
2	<b>Тема 2. Актуальность защиты информации</b> 1) К открытым источникам информации относятся: а) информация, украденная у спецслужб б) газеты, радио, новости в) информация из вскрытого сейфа	б
3	<b>Тема 3. Виды угроз</b> Потенциальные угрозы, против которых направлены технические меры защиты информации: а) потери информации из-за сбоев оборудования, некорректной работы программ и ошибки обслуживающего персонала и пользователей б) потери информации из-за не достаточной установки сигнализации в помещении в) потери информации из-за халатности обслуживающего персонала и не ведения системы наблюдения	а
4	<b>Тема 4. Вредоносное программное обеспечение</b> Для защиты от злоумышленников необходимо использовать: а) системное программное обеспечение б) прикладное программное обеспечение в) антивирусные программы	в
5	<b>Тема 5. Основы законодательства в области информационной безопасности</b> Что относят к правовым мерам: а) средства идентификации и аутентификации пользователей б) охрану вычислительного центра и аппаратуры связи в) разработку норм, устанавливающих ответственность за компьютерные преступления и защиту авторских прав программистов	в
6	<b>Тема 6. Лицензирование и сертификация в информационной безопасности</b> Владельцем информации третьей категории является: а) простые люди б) государство в) коммерческая организация	б
7	<b>Тема 7. Технические средства защиты информации</b> Что является наиболее надежным средством предотвращения потерь компьютерной информации при кратковременном отключении электроэнергии? а) установка источников бесперебойного питания	а

№ п/п	Формулировка задания	Ответ
	б) такого средства не существует в) перекидывать информацию на носитель, который не зависит от энергии	
8	<b>Тема 8. Программно-технические меры защиты информации</b> Программные средства защиты можно разделить на: а) правовые, аппаратные, программные б) административные меры защиты, включающие подготовку и обучение персонала, организацию тестирования и приема в эксплуатацию программ, контроль доступа в помещения и т.д. в) криптография, антивирусные программы, системы разграничения полномочий, средства контроля доступа и т.д.	в

### 10.2.2. Вариант типовых заданий (задач), разработанных в соответствии с установленными этапами формирования компетенций

№ п/п	Условия типовых задач	Ответ
1	Используя шифр Цезаря, зашифруйте фразу: «ПРИШЁЛ УВИДЕЛ ПОБЕДИЛ»	ТУЛЫИОЦЕЛЖЗОТСДЗЖЛО
2	Расшифруйте сообщение, зашифрованное шифром Цезаря, и определите ключ $n$ ( $0 < n < 33$ ), если известно, что исходное сообщение составлено из алфавита АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ: ЧСЮЭЮЪ	$n=16$ ЗВОНОК

### 10.3. Методические материалы, определяющие процедуры оценивания знаний, умений, владений (навыков и (или) практического опыта деятельности), характеризующих этапы формирования компетенций

#### 10.3.1. Условия допуска обучающегося к сдаче зачета и порядок ликвидации академической задолженности

Положение о проведении текущего контроля успеваемости и промежуточной аттестации обучающихся.

#### 10.3.2. Форма проведения промежуточной аттестации по дисциплине

устная  письменная  компьютерное тестирование  иная

#### 10.3.3. Особенности проведения зачета

- Возможность пользоваться конспектом лекций и записями материалов практических занятий.
- Типовые задачи обучающиеся выполняют самостоятельно в рамках подготовки к зачету (варианты заданий сообщаются преподавателем заранее), непосредственно на зачет обучающиеся приходят с готовыми вариантами ответов.
- Время на выполнение тестового задания – 15 минут.
- Время на подготовку к устному собеседованию – 20 минут, на ответ – 10 минут.