

Министерство образования и науки Российской Федерации  
Федеральное государственное бюджетное образовательное учреждение  
высшего профессионального образования



**Пермский национальный исследовательский  
политехнический университет**

Электротехнический факультет  
Кафедра «Автоматика и телемеханика»



**УТВЕРЖДАЮ**

Проректор по учебной работе

*Н. В. Лобов*  
Н. В. Лобов  
2015 г.

**УЧЕБНО-МЕТОДИЧЕСКИЙ КОМПЛЕКС ДИСЦИПЛИНЫ  
«Организация и управление службой защиты информации  
на предприятии»**

Основная образовательная программа подготовки специалистов  
Специальность: 090303.65 «Информационная безопасность автоматизирован-  
ных систем»

**РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ**

<b>Специализация специалиста</b>	09030307.65 «Обеспечение информационной безопасности распределенных информационных систем»		
<b>Квалификация выпускника</b>	специалист		
<b>Специальное звание выпускника</b>	специалист по защите информации		
<b>Выпускающая кафедра</b>	Автоматика и телемеханика		
<b>Форма обучения</b>	очная		
<b>Курс: 4</b>	<b>Семестр(ы): 8</b>		
<b>Трудоёмкость:</b>			
Кредитов по рабочему учебному плану:	5 ЗЕ		
Часов по рабочему учебному плану:	180 ч		
<b>Виды контроля:</b>			
Экзамен: 8 семестр	Зачёт: -	Курсовой проект: -	Курсовая работа: -

Пермь  
2015

**Рабочая программа дисциплины «Организация и управление службой защиты информации на предприятии» разработана на основании:**


- федерального государственного образовательного стандарта высшего профессионального образования утвержденного приказом Министерства образования и науки Российской Федерации от 17 января 2011г. № 60, по направлению подготовки (специальности) 090303 «Информационная безопасность автоматизированных систем» (квалификация (степень) «специалист»);
- компетентностной модели выпускника ООП по специальности 090303.65 - «Информационная безопасность автоматизированных систем», специализации «Обеспечение информационной безопасности распределенных информационных систем», утвержденной 24 июня 2013 г.;
- рабочего учебного плана очной формы обучения по специальности 090303.65 - «Информационная безопасность автоматизированных систем», специализации «Обеспечение информационной безопасности распределенных информационных систем», утвержденного 29 августа 2011 г.

**Рабочая программа согласована** с рабочей программой дисциплин: Внутренний аудит систем защиты информации на соответствие стандартам, Безопасность систем баз данных, Безопасность операционных систем, Управление информационной безопасностью, Безопасность сетей ЭВМ.

Разработчик      доцент


 Саранин Е.И.

Рецензент      канд. техн. наук, доцент

 Шабуров А.С.

**Рабочая программа рассмотрена и одобрена на заседании кафедры «Автоматика и телемеханика»** «17» января 2015 г., протокол № 17.

Заведующий кафедрой,  
«Автоматика и телемеханика»,  
д-р. техн. наук, профессор

 Южаков А.А.

**Рабочая программа одобрена методической комиссией** электротехнического факультета «06» 10 2015г., протокол №\_\_

Председатель методической комиссии  
электротехнического факультета,  
канд. техн. наук, профессор

 Гольдштейн А.Л.

СОГЛАСОВАНО

Начальник управления образовательных программ,  
канд. техн. наук, доцент

 Репецкий Д.С.

## 1 Общие положения

**1.1. Цель дисциплины** – освоение заданных дисциплинарных компетенций в области деятельности по организации и управлению службой защиты информации на предприятии, на основе оценки угроз безопасности информации, технологии организации, кадрового, технологического и нормативно-методического обеспечения, политик безопасности, методах оценки эффективности управления системами защиты информации.

В процессе изучения данной дисциплины студент осваивает следующие дисциплинарные компетенции:

- способность применять методологию научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами (ПК-5);
- способность разрабатывать политики информационной безопасности автоматизированных систем (ПК-20);
- способность участвовать в проектировании системы управления информационной безопасностью автоматизированной системы (ПК-21).

### 1.2 Задачи дисциплины:

#### Изучение:

- методов и средств обеспечения информационной безопасности, механизмов функционирования системы защиты информации на предприятии;
- изучение основных принципов и направлений защиты информации на предприятии, используемых службой защиты информации;
- освоение технологии взаимодействия специалистов по защите информации со службой информационных технологий, а конкретно с системными администраторами и администраторами безопасности систем и сетей, другими подразделениями в системе безопасности;
- изучение теоретических, методологических и практических проблем формирования и функционирования системы защиты информации на предприятиях и в организациях различной формы собственности, в органах власти.

#### формирование умений:

- определения места и значения службы защиты информации в системе безопасности предприятия;
  - установления организационных основ и принципов деятельности службы защиты информации на предприятии, определение целей, функций и задач, которые она решает в процессе создания и управления системами организационной защиты информации на предприятиях с различными организационно-правовыми формами собственности;
  - установления основных требований, предъявляемые к работникам службы защиты информации на предприятии в отношении специальных знаний, а также знаний законодательных и иных нормативных правовых актов, положений, инструкций и других документов, методов и средств, которые работник должен применять при выполнении должностных обязанностей;
- овладение навыками** установления состава мероприятий и последовательности их проведения по созданию службы защиты информации на предприятии.

### 1.3 Предметом освоения дисциплины являются следующие объекты:

- основы организации системы защиты информации на объектовом уровне, порядок и технология создания и реорганизации службы защиты информации, порядок взаимодействия с органами власти и организациями, уполномоченными в области защиты информации, а также предприятиями и организациями по оказанию услуг в области обеспечения информационной безопасности;

- современные проблемы создания и обеспечения функционирования систем защиты информации, организационно-технического и кадрового обеспечения информационной безопасности на предприятии, требования к персоналу;
- технологии построения систем организационного обеспечения защиты информации на предприятии;
- основные методы и технология управления службой защиты информацией в организациях с различными формами собственности;
- цели и функции подразделений по технической защите информации системы защиты информации при создании политики безопасности на предприятии;
- процессы управления системами защиты информации на предприятиях и в организациях с различными организационно-правовыми формами собственности;
- основные методы организационно-технической защиты информации.

#### **1.4 Место дисциплины в структуре профессиональной подготовки выпускников.**

Дисциплина «Организация управления службой защиты информации на предприятии» относится к вариативной части цикла профессиональных дисциплин и является дисциплиной по выбору при освоении ООП по специальности 090303.65 – Информационная безопасность автоматизированных систем.

После изучения дисциплины обучающийся должен освоить части указанных в пункте 1.1 компетенций и продемонстрировать следующие результаты:

**знать:**

- назначение и роль, принципы организации и этапы создания службы защиты информации на предприятии, виды организационных структур службы защиты информации;
- содержание, технологию и порядок организации и реорганизации службы защиты информации на предприятии;
- состав мероприятий и условия, обеспечивающие функционирование службы защиты информации на предприятии;
- порядок кадрового, материально-технического и нормативно-методического обеспечения службы защиты информации на предприятии, должностной состав и функциональные обязанности персонала службы защиты информации на предприятии;
- порядок организации планирования и контроля работ по безопасности службой защиты информации на предприятии;
- методику проведения аудита информационной безопасности на предприятии;

**уметь:**

- определять оптимальную структуру службы защиты информации и разрабатывать направления ее развития;
- обосновывать, организовывать и обеспечивать проведение мероприятий по созданию службы защиты информации;
- осуществлять подбор, расстановку кадров и обучение сотрудников службы защиты информации;
- организовывать работу с персоналом и различных служб предприятия по обеспечению безопасности в работе с конфиденциальной информацией;
- организовывать разработку системы мер по охране персонала, территории, зданий, помещений и продукции предприятий;
- организовывать и осуществлять все виды работ службой защиты информации;
- обеспечивать необходимые условия труда сотрудников службы защиты информации;

- осуществлять управление и контроль за деятельностью сотрудников службы защиты информации и иных подразделений, в которых проводятся мероприятия по технической защите информации;
  - проводить обследование системы защиты информации оценивать эффективность работы службы защиты информации;
  - использовать различные методы проектирования деятельности службы защиты информации на предприятии;
  - выбирать рациональное оборудование и технические средства защиты информации для оснащения рабочих мест сотрудников службы защиты информации;
  - разрабатывать проекты нормативных и организационно-распорядительных документов, регламентирующих работу службы по защите информации на предприятии;
- владеть:**
- методиками оценки эффективности работы службы защиты информации, проведения аудита информационной безопасности на соответствие требованиям безопасности;
  - технологией разработки организационно-функциональной структуры службы защиты информации и комплекса нормативно-методического обеспечения ее деятельности на предприятии.

В таблице 1.1 приведены предшествующие и последующие дисциплины, направленные на формирование компетенций, заявленных в пункте 1.1.

Таблица 1.1 – Дисциплины, направленные на формирование компетенций

Индекс	Наименование компетенции	Предшествующие дисциплины	Последующие дисциплины (группы дисциплин)
<b>Профессиональные компетенции</b>			
ПК-5	способность применять методологию научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами	НИРС, Теория электрических цепей	Подготовка и защита ВКР
ПК-20	способность разрабатывать политики информационной безопасности автоматизированных систем	Безопасность систем баз данных, Безопасность операционных систем	Подготовка и защита ВКР
ПК-21	способность участвовать в проектировании системы управления информационной безопасностью автоматизированной системы	Управление информационной безопасностью, Безопасность сетей ЭВМ.	Подготовка и защита ВКР

## 2 Требования к результатам освоения учебной дисциплины

Учебная дисциплина обеспечивает формирование заданных частей профессиональных компетенций (ПК-5, ПК-20 и ПК-21).

## 2.1 Карты дисциплинарных компетенций

### 2.1.1 Карта дисциплинарной компетенции ПК-5

<b>Индекс ПК-5</b>	<b>Формулировка компетенции:</b> способен применять методологию научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами
------------------------	---

<b>Индекс ПК-5-4</b>	<b>Формулировка дисциплинарной части компетенции:</b> способен применять методологию научных исследований в вопросах организации и управления службой защиты информации на предприятии
--------------------------	---

### 2.1.2 Компонентный состав дисциплинарной компетенции

Перечень компонентов	Виды учебной работы	Средства контроля
<p><b>Знать:</b></p> <ul style="list-style-type: none"> <li>– назначение и роль, принципы организации и этапы создания службы защиты информации на предприятии, виды организационных структур службы защиты информации (ПК-5-4-1з);</li> <li>– содержание, технологию и порядок организации и реорганизации службы защиты информации на предприятии (ПК-5-4-2з);</li> </ul>	Лекции; семинарские и практические занятия; самостоятельное изучение теоретического материала.	Экзамен; отчет по выполнению практических задач, обсуждение результатов самостоятельного изучения теоретического материала в ходе ПЗ и СЗ
<p><b>Уметь:</b></p> <ul style="list-style-type: none"> <li>– определять оптимальную структуру службы защиты информации и разрабатывать направления ее развития (ПК-5-4-1у);</li> <li>– обосновывать, организовывать и обеспечивать проведение мероприятий по созданию службы защиты информации (ПК-5-4-2у);</li> <li>– осуществлять управление и контроль за деятельностью сотрудников службы защиты информации и иных подразделений, в которых проводятся мероприятия по технической защите информации (ПК-5-4-3у);</li> <li>– проводить обследование системы защиты информации оценивать эффективность работы службы защиты информации (ПК-5-4-4у);</li> </ul>	Практические занятия; выполнение индивидуального задания.	Защита отчета по выполнению индивидуального задания.
<p><b>Владеть:</b></p> <ul style="list-style-type: none"> <li>– методиками оценки эффективности работы службы защиты информации, проведения аудита информационной безопасности на соответствие требованиям безопасности (ПК-5-4-1в).</li> </ul>	Выполнение индивидуального комплексного задания.	Защита отчета по индивидуальному комплексному заданию.

### 2.2.1 Карта дисциплинарной компетенции ПК-20

<b>Индекс ПК-20</b>	<b>Формулировка компетенции:</b> способен разрабатывать политики информационной безопасности автоматизированных систем
-------------------------	---

<b>Индекс ПК-20-4</b>	<b>Формулировка дисциплинарной части компетенции:</b> способен разрабатывать политики информационной безопасности автоматизированных систем по вопросам организации и управления службой защиты информации на предприятии
---------------------------	--

### 2.2.2 Компонентный состав дисциплинарной компетенции

Перечень компонентов	Виды учебной работы	Средства контроля
<p><b>Знать:</b></p> <ul style="list-style-type: none"> <li>– состав мероприятий и условия, обеспечивающие функционирование службы защиты информации на предприятии (ПК-20-4-1з);</li> <li>– порядок кадрового, материально-технического и нормативно-методического обеспечения службы защиты информации на предприятии, должностной состав и функциональные обязанности персонала службы защиты информации на предприятии (ПК-20-4-2з);</li> </ul>	Лекции; семинарские и практические занятия; самостоятельное изучение теоретического материала.	Экзамен, отчет по выполнению практических задач, обсуждение результатов самостоятельного изучения теоретического материала в ходе ПЗ и СЗ
<p><b>Уметь:</b></p> <ul style="list-style-type: none"> <li>– осуществлять подбор, расстановку кадров и обучение сотрудников службы защиты информации (ПК-20-4-1у);</li> <li>– организовывать работу с персоналом и различных служб предприятия по обеспечению безопасности в работе с конфиденциальной информацией (ПК-20-4-2у);</li> <li>– организовывать и осуществлять все виды работ службой защиты информации (ПК-20-4-3у);</li> <li>– составлять необходимые отчетные документы по собранным и проанализированным информационным материалам (ПК-20-4-4у);</li> </ul>	Практические занятия; выполнение индивидуального задания.	Защита отчета по выполнению индивидуального задания.
<p><b>Владеть:</b></p> <ul style="list-style-type: none"> <li>– технологией разработки организационно-функциональной структуры службы защиты информации и комплекса нормативно-методического обеспечения ее деятельности на предприятии (ПК-20-4-1в).</li> </ul>	Выполнение индивидуального задания.	Защита отчета по выполнению индивидуального задания.

### 2.2.1 Карта дисциплинарной компетенции ПК-21

<b>Индекс ПК-21</b>	<b>Формулировка компетенции:</b> способен участвовать в проектировании системы управления информационной безопасностью автоматизированной системы
<b>Индекс ПК-21-3</b>	<b>Формулировка дисциплинарной части компетенции:</b> способен участвовать в проектировании системы управления информационной безопасностью автоматизированной системы при организации и управлении службой защиты информации на предприятии

### 2.2.2 Компонентный состав дисциплинарной компетенции

Перечень компонентов	Виды учебной работы	Средства контроля
<p><b>Знать:</b></p> <ul style="list-style-type: none"> <li>– порядок организации планирования и контроля работ по безопасности службой защиты информации на предприятии (ПК-21-3-1з);</li> <li>– методику проведения аудита информационной безопасности на предприятии (ПК-21-3-2з);</li> </ul>	Лекции; семинарские и практические занятия; самостоятельное изучение теоретического материала.	Экзамен, отчет по выполнению практических задач, обсуждение результатов самостоятельного изучения теоретического материала.

		ского материала в ходе ПЗ и СЗ
<b>Уметь:</b> – использовать различные методы проектирования деятельности службы защиты информации на предприятии (ПК-21-1-1у); – выбирать рациональное оборудование и технические средства защиты информации для оснащения рабочих мест сотрудников службы защиты информации (ПК-21-1-2у); – организовывать разработку системы мер по охране персонала, территории, зданий, помещений и продукции предприятий (ПК-21-1-2у); – обеспечивать необходимые условия труда сотрудников службы защиты информации (ПК-21-1-2у);	Практические занятия; выполнение индивидуального задания.	Защита отчета по выполнению индивидуального задания.
<b>Владеть:</b> – технологией разработки организационно-функциональной структуры службы защиты информации и комплекса нормативно-методического обеспечения ее деятельности на предприятии (ПК-21-1-1в).	Выполнение индивидуального задания.	Защита отчета по выполнению индивидуального задания.

### 3. Структура учебной дисциплины по видам и формам учебной работы

Структура дисциплины содержит распределение используемых видов аудиторной работы (АРС) и самостоятельной работы студентов (СРС) с указанием трудоемкости и форм представления результатов выполнения видов учебных работ.

3.2. Основными видами аудиторной работы по дисциплине являются:

- лекции (Л);
- практические занятия (ПЗ)
- семинарские занятия (СЗ).

3.3. Основными видами самостоятельной работы по дисциплине являются:

- самостоятельное изучение теоретического материала (ИТМ);
- выполнение индивидуального задания по учебному модулю дисциплины (ИЗМ).

3.4. Структура дисциплины по видам и формам приведена в табл. 3.1.

Таблица 3.1 – Структура дисциплины по объемам и видам учебной работы

№ п.п.	Виды учебной работы	Трудоёмкость, ч	Форма представления результатов
1	2	3	4
1	<b>Аудиторная работа</b>	<b>72</b>	
	- в том числе в интерактивной форме	32	
	- лекции (Л)	32	конспект лекций
	- в том числе в интерактивной форме	16	
	- практические занятия (ПЗ), семинарские занятия (СЗ)	36	отчёт о выполнении
	- в том числе в интерактивной форме	16	
	Контроль самостоятельной работы (КСР)	4	
2	<b>Самостоятельная работа студентов (СРС)</b>	<b>72</b>	



	- самостоятельное изучение теоретического материала (ИТМ)	36	отчет по вопросам для текущего и рубежного контроля
	- выполнение индивидуальных заданий по модулю (ИЗМ)	36	отчёт о выполнении
3	Итоговая аттестация по дисциплине	<b>36</b>	<b>Экзамен</b>
4	<b>Трудоёмкость дисциплины, всего:</b> <b>в часах (ч)</b> <b>в зачётных единицах (ЗЕ)</b>	<b>180</b> <b>5</b>	

## 4 Содержание учебной дисциплины

### 4.1 Модульный тематический план

Таблица 4.1 – Тематический план по модулям учебной дисциплины

Номер учебного модуля	Номер раздела дисциплины	Номер темы дисциплины	Количество часов (очная форма обучения)							Итог. аттест.	Трудоёмкость АЧ/ЗЕТ	
			Аудиторная работа студента (АРС)				Самостоятельная работа студента (СРС)					
			Всего	Лк	ПЗ, СЗ	КСР	Всего	ИТМ	ИЗМ			
1	2	3	4	5	6	7	8	9	10	11	12	
1	1	1	4	2	2		4	2	2			8
		2	6	2	4		4	2	2			10
		3	8	4	4		8	4	4			16
		4	9	4	4	1	8	4	4			17
		<b>Всего по модулю:</b>	<b>27</b>	12	14	1	<b>24</b>	12	12			<b>51</b>
2	2	5	6	4	2		8	4	4			14
		6	6	2	4		8	4	4			14
		7	7	2	4	1	8	4	4			15
		<b>Всего по модулю:</b>	<b>19</b>	8	10	1	<b>24</b>	12	12			<b>43</b>
3	3	8	4	2	2		4	2	2			8
		9	4	2	2		4	2	2			8
		10	4	2	2		4	2	2			8
		11	4	2	2		4	2	2			8
		12	10	4	4	2	8	4	4			18
<b>Всего по модулю:</b>	<b>26</b>	12	12	2	<b>24</b>	12	12			<b>50</b>		
Итоговая аттестация												<b>36</b>
Итого			<b>72</b>	<b>32</b>	<b>36</b>	<b>4</b>	<b>72</b>	<b>36</b>	<b>36</b>	<b>36</b>		<b>180/5</b>

### 4.2. Содержание разделов и тем учебной дисциплины

Модуль 1. Концептуальные основы создания службы защиты информации и определения объектов защиты на предприятии.

Раздел 1. Концептуальные основы создания службы защиты информации и определения объектов защиты.

АРС: Л - 12 ч., ПЗ, СЗ - 14 ч., КСР – 1 ч., СРС: ИТМ - 12 ч., ИЗМ (ИЗМ-1) - 12 ч.

**Тема 1. Введение в дисциплину. Сущность управления защитой информации на предприятии и принципы ее организации.** Цель, задачи дисциплины, значение ее для подготовки специалиста. Знания и умения студентов, которые должны быть получены в результате ее изучения. Понятие, сущность и назначение, основные направления деятельности по созданию системы защиты информации, решаемые с ее созданием задачи по экономической и информационной безопасности и в целом обеспечения деятельности предприятия. Принципы управления и средства защиты информации на предприятии.

**Тема 2. Правовые, методологические и концептуальные основы создания службы защиты информации.** Назначение службы защиты информации. Место службы защиты информации в системе безопасности предприятия. Служба защиты информации как составная часть системы безопасности. Служба защиты информации как орган управления и координации деятельности по обеспечению безопасности. Служба защиты информации как координатор деятельности по обеспечению безопасности информации. Статус службы защиты информации в структуре предприятия.

**Тема 3. Определение задач и функций службы защиты информации.** Организационные задачи и функции службы защиты информации. Технологические задачи и функции службы защиты информации. Координационные задачи и функции службы защиты информации. Взаимосвязь и соотношение организационных, технологических и координационных задач и функций. Факторы, влияющие на определение задач и функций службы защиты информации.

**Тема 4. Определение организационной структуры и штата службы защиты информации.**

Общая структурная схема службы защиты информации. Подразделения службы защиты информации. Факторы, определяющие конкретную структуру службы защиты информации. Централизованная и децентрализованная структуры службы защиты информации, условия, критерии, определяющие выбор структур. Должностной состав сотрудников службы защиты информации, его зависимость от характера выполняемых работ. Задачи, функции, права и ответственность заместителя (помощника) руководителя предприятия по безопасности в области защиты информации. Задачи, функции, права и ответственность руководителя службы защиты информации, его заместителей, руководителей подразделений службы защиты, функции сотрудников и уполномоченных службы защиты информации. Факторы, определяющие численность сотрудников службы защиты информации.

**Модуль 2. Организация деятельности службы защиты информации на предприятии.**  
**Раздел 2. Организация деятельности службы защиты информации на предприятии.**  
 АРС: Л - 8 ч, ПЗ, СЗ - 10 ч., КСР - 1 ч., СРС: ИТМ - 12 ч., ИЗМ (ИЗМ-1) - 12 ч.

**Тема 5. Организационные основы и принципы деятельности службы защиты информации.** Порядок создания службы защиты информации. Структура и содержание положения о службе защиты информации. Состав и содержание других нормативных документов, регламентирующих деятельность службы защиты информации. Основные принципы организации и деятельности службы защиты информации. Условия и факторы, влияющие на организацию работы службы защиты информации. Организация взаимодействия службы защиты информации со структурными подразделениями предприятия и организациями-лицензиатами в области оказания услуг по защите информации.

**Тема 6. Подбор, расстановка и обучение сотрудников службы защиты информации.** Общие и специфические требования, предъявляемые к сотрудникам службы защиты инфор-

магии. Особенности подбора кадров. Методы получения информации о кандидатурах на должности. Социально-психологические факторы, влияющие на расстановку кадров. Формы создания и способы поддержания необходимого микроклимата в коллективе. Формы повышения квалификации сотрудников. Подготовка кадрового резерва.

**Тема 7. Организация труда сотрудников службы защиты информации.** Специфика деятельности сотрудников службы защиты информации. Распределение обязанностей между сотрудниками службы защиты информации. Обеспечение персональной ответственности за сохранность носителей информации. Структура и содержание должностных инструкций сотрудников службы защиты информации. Организация рабочих мест сотрудников службы защиты информации (рациональное размещение, оснащение оборудованием, техническими средствами). Обеспечение необходимых условий труда. Охрана труда. Культура труда. Карты организации трудового процесса.

**Модуль 3. Особенности построения и управления службой защиты информации предприятия и оценка эффективности ее работы.**

**Раздел 3. Особенности построения и управления службой защиты информации предприятия и оценка эффективности ее работы**

АРС: Л - 12 ч, ПЗ, СЗ - 12 ч., КСР - 2 ч., СРС: ИТМ - 12 ч., ИЗМ (ИЗМ-1) - 12 ч.

**Тема 8. Принципы и методы управления службой защиты информации.** Принципы управления службой защиты информации. Понятие и сущность методов управления. Система методов управления. Административно-правовые методы управления. Экономические методы управления. Социально-психологические методы управления. Взаимосвязь методов управления. Необходимость комплексного и системного применения методов управления службой защиты информации.

**Тема 9. Кадровое, материально-техническое и нормативно-методическое обеспечение службы защиты информации.** Кадровое обеспечение службы защиты информации. Распределение функций по защите информации между специалистом по защите информации, администратором безопасности и системным администратором. Материально-техническое обеспечение защиты информации. Нормативно-методическое обеспечение деятельности службы защиты информации на предприятии. Порядок разработки нормативных и организационно-распорядительных документов, регламентирующих работу по защите информации на предприятии.

**Тема 10. Технология управления службой защиты информации.** Планирование и контроль организации работ по защите информации специалистами службы защиты информации. Состав и содержание управленческих функций. Технология управления службой защиты информации. Значение управленческих решений. Цели планирования. Виды планирования, их назначение. Содержание и структура планов. Технология планирования. Организация выполнения планов. Методы и формы контроля выполнения планов. Основные контрольные мероприятия по защите информации.

**Тема 11. Оценка эффективности службы защиты информации.** Понятие эффективности и определение эффективности защиты информации. Требования по защите информации. Подходы к оценке эффективности и результатов деятельности службы защиты информации. Критерии эффективности службы защиты информации. Способы повышения эффективности управления службой защиты информации. Проведение аудита информационной безопасности на предприятии.

**Тема 12. Методы оргпроектирования деятельности службы защиты информации.** Общая характеристика методов оргпроектирования. Цели и назначение методов оргпроектирования. Классификация научно-исследовательских методов оргпроектирования. Методы исследования в оргпроектировании. Методы обследования (сбора исходных данных) системы защиты информации и службы защиты информации. Методы количественно-качественного анализа и синтеза полученной информации о деятельности службы. Методы проектирования организации и технологии деятельности службы защиты информации.

### 4.3. Перечень тем практических занятий

Таблица 4.4 – Темы практических занятий (семинаров)

№ п/п	Номер темы дисциплины	Наименование темы практического (семинарского) занятия
1	1	Объекты защиты информации на предприятии, применение методов защиты информации для формирования концепции информационной безопасности предприятия (СЗ)
2	2	Правовое и нормативно-методическое обеспечение деятельности службы защиты информации на предприятии (ПЗ)
3	3	Структура и основное содержание концепции информационной безопасности предприятия, содержание Руководства по ПДИТР (ПЗ)
4	4	Организация работ по формированию системы производственного контроля обеспечения защиты информации на предприятии (СЗ)
5	5	Организация взаимодействия в решении задач обеспечения безопасности информационных активов службой защиты информации (СЗ)
6	6	Организация взаимодействия в решении проблем ТЗИ администратора безопасности, системного администратора и специалиста по защите информации (ПЗ)
7	7	Компетентностные уровни профессионалов в области информационной безопасности. (СЗ)
8	7	Организация защиты информации при приеме посетителей и командированных, режимные меры при посещении иностранными представителями (СЗ)
9	8	Состав режимных мер и особенности оборудования защищаемых помещений для проведения работ с использованием сведений конфиденциального характера (ПЗ)
10	9	Разработка нормативных и организационно-распорядительных документов, регламентирующих проведение мероприятий при передаче информации ограниченного доступа и снятии ограничений на ознакомление (ПЗ)
11	10	Профессиональные компетенции специалиста по защите информации в области управления рисками и инцидентами информационной безопасности (СЗ)
12	11	Профессиональные компетенции специалиста по защите информации в области компьютерной форензики. (СЗ)
13	12	Применение методов оценки эффективности систем защиты информации. Методики проведения аудита информационной безопасности. (ПЗ)
14	12	Особенности применения нормативно - правовых актов и методик защиты информации при построении систем защиты информации с учетом современных тенденций развития бизнеса и информационных технологий (СЗ)

### 4.4. Перечень тем лабораторных работ

Не предусмотрены.

## 4.5 Виды самостоятельной работы студентов

Таблица 4.5 – Виды самостоятельной работы студентов (СРС)

Номер темы (раздела) дисциплины	Вид самостоятельной работы студентов	Трудоёмкость, часов
1	ИТМ: Знания и умения студентов, которые должны быть получены в результате изучения дисциплины	2
2	ИТМ: Характер и степень влияния различных факторов на организацию системы защиты информации	2
3	ИТМ: Порядок организации нормативного закрепления информации ограниченного доступа	4
4	ИТМ: Особенности помещений как объектов защиты	4
4	ИЗМ: В соответствии с заданием для модуля 1, п.п. 4.5.1	12
5	ИТМ: Базовые модели угроз безопасности различных видов информации ограниченного доступа	4
6	ИТМ: Методы «социального инжиниринга»	4
7	ИТМ: Формальные модели безопасности	4
7	ИЗМ: В соответствии с заданием для модуля 2, п.п. 4.5.1	12
8	ИТМ: Аprobация системы защиты информации и ввод ее в эксплуатацию	2
9	ИТМ: Порядок разработки нормативных и организационно-распорядительных документов, регламентирующих работу по защите информации на предприятии	2
10	ИТМ: Основные контрольные мероприятия по защите информации	2
11	ИТМ: Области применения различных методов и моделей для решения задач оценки эффективности системы защиты информации на предприятии	2
12	ИТМ: Основы проведения поисковых мероприятий по выявлению скрытых устройств	4
12	ИЗМ: В соответствии с заданием для модуля 3, п.п. 4.5.1	12
	Итого: в ч / в ЗЕ	<b>72/2</b>

### 4.5.1. Темы для выполнения индивидуального задания по модулю (ИЗМ)

Индивидуальное задание представляет собой разрабатываемый студентом отчет по вопросам организации и управления службой защиты информации на предприятии. Темы изучаются студентом самостоятельно, в течение всего учебного семестра и отражает необходимые требования по основным задачам, решаемым в процессе организации и управления подразделением, обеспечивающим информационную безопасность предприятия. Последовательность разработки тем осуществляется поэтапно, в соответствии с последовательностью изучаемых разделов учебной дисциплины.

#### Раздел 1, модуль 1

**Тема 1.** Определение основных видов угроз безопасности на предприятии.

**Тема 2.** Определение характера происхождения угроз безопасности информации.

**Тема 3.** Определение порядка проведения основных мероприятий по безопасности на предприятии и включение их в Руководство по защите информации.

**Тема 4.** Определение мероприятий системы производственного контроля, обеспечивающих достаточный уровень защиты и безопасности информации на предприятии.

#### Раздел 2, модуль 2

**Тема 5.** Разработка рекомендаций повышающих уровень защищенности объектов информатизации на предприятии.

- Тема 6.** Разработка практических рекомендаций по организации взаимодействия в решении проблем ТЗИ основных специалистов в области безопасности информационных систем.
- Тема 7.** Разработка должностных инструкций в соответствии с квалификационными характеристиками для руководителей и специалистов службы защиты информации.
- Раздел 3, модуль 3**
- Тема 8.** Разработка регламентов обеспечения режимных требований при посещении предприятия представителями иностранных государств.
- Тема 9.** Разработка комплекта организационно-распорядительных документов, регламентирующих работу со сведениями конфиденциального характера.
- Тема 10.** Разработка мероприятий по защите информации в защищаемых помещениях на предприятии.
- Тема 11.** Разработка планов проведения работ по пресечению инцидентов информационной безопасности и контрольных мероприятий службой защиты информации.
- Тема 12.** Разработка мероприятий системы аудита информационной безопасности на предприятии.

#### **4.5.2 Перечень тем курсовых работ (проектов)**

Не предусмотрены.

### **5 Образовательные технологии, используемые для формирования компетенций**

Проведение лекционных занятий по дисциплине основывается на активном методе обучения, при которой учащиеся не пассивные слушатели, а активные участники занятия, отвечающие на вопросы преподавателя. Вопросы преподавателя нацелены на активизацию процессов усвоения материала. Преподаватель заранее намечает список вопросов, стимулирующих ассоциативное мышление и установления связей с ранее освоенным материалом.

Проведение семинарских и практических занятий основывается на интерактивной форме взаимодействия преподавателя и студентов между собой. Преподавателем предлагается проблема (ситуация, условия, ограничения, конкретный пример), и путем обсуждения находится решение. Место преподавателя в интерактивных занятиях сводится к направлению деятельности учащихся на достижение целей занятия. Проведение практических занятий основывается на активном применении обучаемыми студентами руководящих и нормативно-методических документов ФСТЭК России, рекомендаций по применению современных методов и средств защиты информации.

## **6. Управление и контроль освоения компетенций**

### **6.1 Текущий контроль освоения заданных дисциплинарных компетенций**

Текущий контроль освоения дисциплинарных компетенций проводится в следующих формах:

- текущий опрос, текущая проверочная работа для анализа усвоения материала предыдущей лекции (ТО);
- оценка работы студента на лекционных, практических и семинарских занятиях в рамках рейтинговой системы.

### **6.2 Рубежный и промежуточный контроль освоения заданных дисциплинарных компетенций**

Рубежный контроль освоения дисциплинарных компетенций проводится по окончании модулей дисциплины в следующих формах:

- отчет за индивидуальное задание по модулю (модуль 1, 2, 3);
- тест для рубежного контроля (модуль 1, 2, 3) (РТ).

### 6.3 Итоговый контроль освоения заданных дисциплинарных компетенций

#### 1) Экзамен

Итоговый контроль уровня освоения заданных дисциплинарных компетенций производится в виде экзамена. Допуск к экзамену по дисциплине предоставляется по итогам проведения рубежного контроля по выполнению индивидуальных заданий по модулю, результатам практических и семинарских занятий.

Экзамен по дисциплине проводится в виде ответа на вопросы билета. Билет содержит два теоретических вопроса.

Фонды оценочных средств, включающий задания практических занятий, тестовые задания для рубежного контроля и методы оценки, критерии оценивания, перечень контрольных точек и таблица планирования результатов обучения, вопросы к экзамену, позволяющие оценить результаты освоения данной дисциплины, входит в состав УМКД на правах отдельного документа.

### 6.4 Виды и формы текущего, рубежного и итогового контроля освоения элементов и частей компетенций

Таблица 6.1 - Виды контроля освоения элементов и частей компетенций

Контролируемые результаты освоения дисциплины (ЗУВы)	Вид/форма контроля				
	ТО	РТ	ОПЗ	ОИЗМ	Экз.
<b>В результате освоения дисциплины студент</b>					
<b>Знает:</b>					
– назначение и роль, принципы организации и этапы создания службы защиты информации на предприятии, виды организационных структур службы защиты информации (ПК-5-4-1з);	+	+	+		+
– содержание, технологию и порядок организации и реорганизации службы защиты информации на предприятии (ПК-5-4-2з);	+	+	+		+
– состав мероприятий и условия, обеспечивающие функционирование службы защиты информации на предприятии (ПК-20-4-1з);	+	+	+		+
– порядок кадрового, материально-технического и нормативно-методического обеспечения службы защиты информации на предприятии, должностной состав и функциональные обязанности персонала службы защиты информации на предприятии (ПК-20-4-2з);	+	+	+		+
порядок организации планирования и контроля работ по безопасности службой защиты информации на предприятии (ПК-21-3-1з);	+	+	+		+
– методику проведения аудита информационной безопасности на предприятии (ПК-21-3-2з);	+	+	+		+

<p><b>Умеет:</b></p> <ul style="list-style-type: none"> <li>– определять оптимальную структуру службы защиты информации и разрабатывать направления ее развития (ПК-5-4-1у);</li> <li>– обосновывать, организовывать и обеспечивать проведение мероприятий по созданию службы защиты информации (ПК-5-4-2у);</li> <li>– осуществлять управление и контроль за деятельностью сотрудников службы защиты информации и иных подразделений, в которых проводятся мероприятия по технической защите информации (ПК-5-4-3у);</li> <li>– проводить обследование системы защиты информации оценивать эффективность работы службы защиты информации (ПК-5-4-4у);</li> <li>– осуществлять подбор, расстановку кадров и обучение сотрудников службы защиты информации (ПК-20-4-1у);</li> <li>– организовывать работу с персоналом и различных служб предприятия по обеспечению безопасности в работе с конфиденциальной информацией (ПК-20-4-2у);</li> <li>– организовывать и осуществлять все виды работ службой защиты информации (ПК-20-4-3у);</li> <li>– составлять необходимые отчетные документы по собранным и проанализированным информационным материалам (ПК-20-4-4у);</li> <li>– использовать различные методы проектирования деятельности службы защиты информации на предприятии (ПК-21-1-1у);</li> <li>– выбирать рациональное оборудование и технические средства защиты информации для оснащения рабочих мест сотрудников службы защиты информации (ПК-21-1-2у);</li> <li>– организовывать разработку системы мер по охране персонала, территории, зданий, помещений и продукции предприятий (ПК-21-1-2у);</li> <li>– обеспечивать необходимые условия труда сотрудников службы защиты информации (ПК-21-1-2у);</li> </ul>			+	+	
<p><b>Владеет:</b></p> <ul style="list-style-type: none"> <li>– методиками оценки эффективности работы службы защиты информации, проведения аудита информационной безопасности на соответствие требованиям безопасности (ПК-5-4-1в)</li> <li>– технологией разработки организационно-функциональной структуры службы защиты информации и комплекса нормативно-методического обеспечения ее деятельности на предприятии (ПК-20-4-1в).</li> </ul>			+	+	

ТО – текущий опрос (контроль знаний по теме);

РТ – рубежное тестирование по модулю (автоматизированная система контроля знаний);

ОПЗ – отчет по практическому заданию на групповых занятиях (оценка умений и владений);

ОИЗМ – отчет по выполнению индивидуального задания по модулю (оценка умений и владений);

Экз. – (оценка знаний).



## 7. График учебного процесса по дисциплине

Таблица 7.1 – График учебного процесса по дисциплине

Виды работ	Распределение часов по учебным неделям																		Итого, ч
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	
<b>Раздел:</b>	<b>1</b>						<b>2</b>					<b>3</b>							
Лекции	2	2	2	2	2	2	2	2	2	2		2	2	2	2	2	2		<b>32</b>
Практические, семинарские занятия (ПЗ, СЗ)	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	<b>36</b>
Самост. изучение теоретического материала	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	<b>36</b>
Вып. инд. заданий (ИЗМ)	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	<b>36</b>
КСР							1					1						2	<b>4</b>
<b>Модуль:</b>	<b>1</b>						<b>2</b>					<b>3</b>							
Контр. тестирование							+					+						+	
Дисциплин. контроль																			<b>Экз.</b>

## 8. Учебно-методическое и информационное обеспечение дисциплины

### 8.1. Карта обеспеченности дисциплины учебно-методической литературой

Организация и управление  
службой защиты информа-  
ции  
на предприятии

*полное название дисциплины*

Профессиональный цикл

обязат.  
 по выбору  
студента

базовая часть  
цикла  
 вариативная  
часть цикла

090303.65

*код направления / специаль-  
ности*

*сти*

«Информационная безопасность автоматизирован-  
ных систем», специализация «Обеспечение информаци-  
онной безопасности распределенных информационных  
систем»

*полное название направления/ специальности*

КОБ/КОБ

Уровень  специалист  
подготовки  бакалавр  
 магистр

Форма  очная  
обучения  заочная  
 очно-заочная

2015

семестр(ы) 8

количество групп  
количество студентов

1  
20

Саранин Евгений Ильич, доцент,  
электротехнический факультет,  
кафедра АТ, телефон: 239-18-16.

## СПИСОК ИЗДАНИЙ

№	Библиографическое описание	Количество экземпляров в библиотеке
1	2	3
<b>1. Основная литература</b>		
1	Грибунин В.Г. Комплексная система защиты информации на предприятии : учебное пособие для вузов / В.Г. Грибунин В.В. Чудовский .— Москва : Академия, 2009 .— 412 с.	23
2	Гришина Н.В. Организация комплексной системы защиты информации / Н. В. Гришина.— М. : Гелиос АРВ, 2007 .— 255 с.	10
3	Милославская Н.Г. Технические, организационные и кадровые аспекты управления информационной безопасностью : учебное пособие для вузов / Н. Г. Милославская, М. Ю. Сенаторов, А. И. Толстой .— Москва : Горячая линия-Телеком, 2012 .— 214 с.	5
<b>2. Дополнительная литература</b>		
<b>2.1. Учебные и научные издания</b>		
1	Садердинов А. А. Информационная безопасность предприятия : учебное пособие / А. А. Садердинов, В. А. Трайнев, А. А. Федулов ; Международная академия наук информации, информационных процессов и технологий.— Москва : Дашков и К, 2004 .— 336 с.	14
2	Северин В.А. Правовая защита информации в коммерческих организациях: учебное пособие для вузов / В.А. Северин; Под ред. Б.И. Пугинского.— Москва: Академия, 2009 .— 220 с.	4
3	Игнатъев В.А. Защита информации в корпоративных информационно-вычислительных сетях: монография / В. А. Игнатъев.— Старый Оскол: ТНТ, 2005.— 550 с.	1

**Основные данные об обеспеченности на** \_\_\_\_\_  
(дата составления рабочей программы)

Основная литература  обеспечена  не обеспечена

Дополнительная литература  обеспечена  не обеспечена

Зав. отделом комплектования  
научной библиотеки \_\_\_\_\_ Н. В. Тюрикова

**Текущие данные об обеспеченности на** \_\_\_\_\_  
(дата контроля литературы)

Основная литература  обеспечена  не обеспечена

Дополнительная литература  обеспечена  не обеспечена

Зав. отделом комплектования  
научной библиотеки \_\_\_\_\_ Н.В. Тюрикова

## 8.2 Компьютерные обучающие и контролирующие программы

Таблица 8.1 – Используемые компьютерные обучающие программы

№ п/п	Вид учебного занятия	Наименование программного продукта	Рег. номер	Назначение
1	2	3	4	5
1	ПЗ, СЗ	Базы данных правовой информации – Информационно-правового обеспечения “Гарант” - www.garant.ru; – Справочно-правовой системы “Консультант Плюс” - www.consultant.ru.	б/н	

## 8.3 Программные инструментальные средства

Презентационные материалы для лекционных занятий

## 8.4 Аудио- и видео-пособия

Не предусмотрены

## 9 Материально-техническое обеспечение дисциплины

### 9.1 Специализированные лаборатории и классы

Таблица 9.1 – Специализированные лаборатории и классы

№ п.п.	Помещения			Площадь, м <sup>2</sup>	Количество посадочных мест
	Название	Принадлежность (кафедра)	Номер аудитории		
1	2	3	4	5	6
1	Дисплейный класс	Кафедра АТ	308 корп. А	34	18

### 9.2 Основное учебное оборудование

Таблица 9.2 – Учебное оборудование

№ п.п.	Наименование и марка оборудования (стенда, макета, плаката)	Кол-во, ед.	Форма приобретения / владения (собственность, оперативное управление, аренда и т.п.)	Номер аудитории
1	2	3	4	5
1	ПК Intel Pentium Dual CPU 2000 МГц	6	Оперативное управление	308 корп. А

**Лист регистрации изменений**

№ п.п.	Содержание изменения	Дата, номер протокола заседания кафед- ры
1.		
2.		
3.		
4.		
5.		

3+

Министерство образования и науки Российской Федерации  
Федеральное государственное бюджетное образовательное учреждение  
высшего образования



**«Пермский национальный исследовательский  
политехнический университет»  
Электротехнический факультет  
Кафедра «Автоматика и телемеханика»**

**УТВЕРЖДАЮ**

Заведующий кафедрой  
«Автоматика и телемеханика»  
д-р техн. наук, проф.

\_\_\_\_\_ А.А. Южаков  
Протокол заседания кафедры АТ  
от «16» \_\_\_\_\_ 01 \_\_\_\_\_ 2017 г. № 18

**УЧЕБНО-МЕТОДИЧЕСКИЙ КОМПЛЕКС ДИСЦИПЛИНЫ  
«Организация и управление службой защиты информации  
на предприятии»  
РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ**

<b>Специальность:</b>	10.05.03 Информационная безопасность автоматизированных систем
<b>Специализация программы специалитета:</b>	Обеспечение информационной безопасности распределенных информационных систем
<b>Квалификация выпускника:</b>	специалист по защите информации
<b>Выпускающая кафедра:</b>	Автоматика и телемеханика
<b>Форма обучения:</b>	очная

**Курс: 4      Семестр: 8**

**Трудоемкость:**

Кредитов по базовому учебному плану (БУП):  
Часов по базовому учебному плану (БУП):

5  
180

**Виды контроля:**

Экзамен: - **8**      Зачет: - **нет**      Курсовой проект: - **нет**      Курсовая работа: - **нет**

Пермь 2017 г.

**Рабочая программа дисциплины «Организация и управление службой защиты информации на предприятии» разработана на основании:**

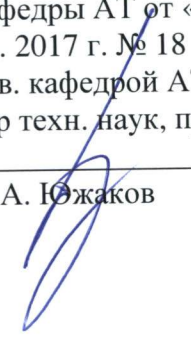
- Федерального государственного образовательного стандарта высшего образования по специальности 10.05.03 Информационная безопасность автоматизированных систем (уровень специалитета), утвержденного приказом Министерства образования и науки Российской Федерации от «01» декабря 2016 г. № 1509;

- Компетентностной модели выпускника образовательной программы высшего образования – программы по специальности 10.05.03 Информационная безопасность автоматизированных систем, специализации «Обеспечение информационной безопасности распределенных информационных систем», утвержденной «24» июня 2013 г. (с изменениями, в связи с переходом на ФГОС ВО);

- Базового учебного плана очной формы обучения образовательной программы высшего образования – программы по специальности 10.05.03 Информационная безопасность автоматизированных систем, специализации «Обеспечение информационной безопасности распределенных информационных систем», утвержденного «22» декабря 2016 г.

**Рабочая программа согласована с рабочими программами дисциплин, участвующих в формировании компетенций и их составляющих, приобретение которых является целью данной дисциплины:** Защита и обработка конфиденциальных документов, Информационная безопасность в банковской системе, Внутренний аудит систем защиты информации на соответствие стандартам, Аудит информационной безопасности, Методы проектирования защищенных распределенных информационных систем базового учебного плана образовательной программы высшего образования - программы по специальности 10.05.03 Информационная безопасность автоматизированных систем, специализации Обеспечение информационной безопасности распределенных информационных систем.

### Лист регистрации изменений

№ п.п	Содержание изменения	Дата, номер протокола заседания кафедры. Подпись заведующего кафедрой
1.	<p>Содержание стр. 1, кроме абзацев 6-9, изложить в редакции, приведенной на стр. 1а.</p> <p>Содержание стр. 2 (абзацы 1-5) изложить в редакции, приведенной на стр. 2а.</p> <p><b>Изменения шифров и формулировок компетенций (стр. 3, 5-8, 9-14, 28-35) внесены на основании перехода на ФГОС ВО по направлению подготовки (специальности) 10.05.03 Информационная безопасность автоматизированных систем (квалификация (степень) «специалист»), утвержденного приказом Министерства образования и науки Российской Федерации от «01» декабря 2016 г. № 1509;</b></p> <ul style="list-style-type: none"> <li>- объединение профессиональных компетенций ПК-5 и ПК-20 считать профессиональной компетенцией <b>ПК-3</b>, с формулировкой «Способностью проводить анализ защищенности автоматизированных систем»;</li> <li>- изменить шифр дисциплинарных компетенций с ПК-5.С3.ДВ.3.1 и ПК-20.С3.ДВ.3.1 на ПК-3.Б1.ДВ.06.1</li> <li>- профессиональную компетенцию ПК-21 считать профессиональной компетенцией <b>ПСК-7.5</b> с формулировкой «Способностью координировать деятельность подразделений и специалистов по защите информации в организациях, в том числе на предприятии и в учреждении»;</li> <li>- изменить шифр дисциплинарной компетенции с ПК-21.С3.ДВ.3.1 на ПСК- 7.5.Б1.ДВ.06.1</li> </ul> <p>Наименование раздела 1.4 «Место учебной дисциплины в структуре профессиональной подготовки выпускников» изложить в следующей редакции: «Место учебной дисциплины в структуре образовательной программы».</p> <p>В первом абзаце раздела 1.4 заменить слова «цикла профессиональных дисциплин» на «блока 1. Дисциплины (модули)».</p> <p>Наименование раздела 2 «Требования к результатам освоения учебной дисциплины» изложить в следующей редакции: «Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы».</p> <p>раздел 3 «Структура учебной дисциплины по видам и формам учебной работы» дополнить новым абзацем следующего содержания: «Объем дисциплины в зачетных единицах составляет 5 ЗЕ. Количество часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся указано в таблице 3.1.».</p>	<p>Протокол заседания кафедры АТ от «16» 01. 2017 г. № 18 Зав. кафедрой АТ д-р техн. наук, проф.</p> <p>_____</p> <p>А.А. Южаков</p> 



<p>В табл. 3.1.:</p> <p>а) строку п. 1 дополнить словами «(контактная работа)»;</p> <p>б) строку п. 3 изложить в следующей редакции: «Итоговый контроль (промежуточная аттестация обучающихся) по дисциплине:».</p>	
<p>В табл. 4.1.:</p> <p>а) в строке п. 1 «Количество часов (очная форма обучения)» дополнить словами «и виды занятий»;</p> <p>б) «Итоговая аттестация» заменить на «Итоговый контроль (промежуточная аттестация).</p>	
<p>В раздел 4.4 «Распределение тем по видам самостоятельной работы» добавить параграф с наименованием «Методические указания для обучающихся по изучению дисциплины» следующего содержания:</p> <p>«При изучении дисциплины обучающимся целесообразно выполнять следующие рекомендации:</p> <ol style="list-style-type: none"> <li>1. Изучение учебной дисциплины должно вестись систематически.</li> <li>2. После изучения какого-либо раздела по учебнику или конспектным материалам рекомендуется по памяти воспроизвести основные термины, определения, понятия раздела.</li> <li>3. Особое внимание следует уделить выполнению отчетов по практическим занятиям, лабораторным работам и индивидуальным комплексным заданиям на самостоятельную работу.</li> <li>4. Изучение дисциплины осуществляется в течение одного семестра, график изучения дисциплины приводится п. 7.</li> <li>5. Вся тематика вопросов, изучаемых самостоятельно, задается на лекциях преподавателем. Им же даются источники (в первую очередь вновь изданные в периодической научной литературе) для более детального понимания вопросов, озвученных на лекции.» </li></ol>	
<p>Наименование раздела 6 изложить в следующей редакции:</p> <p>«Фонд оценочных средств дисциплины».</p>	
<p>Наименование параграфа 6.1 изложить в редакции «Текущий и рубежный контроль освоения заданных дисциплинарных частей компетенций».</p>	
<p>В параграф 6.1 добавить первый абзац следующего содержания: «Текущий контроль осуществляется путем устного опроса во время аудиторных занятий».</p>	
<p>Наименование раздела 8 Учебно-методическое и информационное обеспечение дисциплины» изложить в следующей редакции: «Перечень учебно-методического и информационного обеспечения для самостоятельной работы обучающихся по дисциплине».</p>	
<p>Изменить название раздела «Список изданий» на «8.2. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины».</p>	
<p>Добавить в таблицу 8.1 строку «2.5 Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины».</p>	
<p>Дополнить п. 2.5 таблицы строками:</p> <p><b>Электронная библиотека</b> Научной библиотеки Пермского</p>	

	<p>национального исследовательского политехнического университета [Электронный ресурс : полнотекстовая база данных электрон. документов изданных в Изд-ве ПНИПУ]. – Электрон. дан. (1 912 записей). – Пермь, 2014. – Режим доступа: <a href="http://elib.pstu.ru/">http://elib.pstu.ru/</a>. – Загл. с экрана.</p> <p><b>Лань</b> [Электронный ресурс : электрон.-библ. система : полнотекстовая база данных электрон. документов по гуманитар., естеств., и техн. наукам] / Изд-во «Лань». – Санкт-Петербург : Лань, 2010- . – Режим доступа: <a href="http://e.lanbook.com/">http://e.lanbook.com/</a>. – Загл. с экрана.</p> <p><b>Консультант Плюс</b> [Электронный ресурс : справочная правовая система : документы и комментарии : универсал. информ. ресурс]. – Версия Проф, сетевая. – Москва, 1992. – Режим доступа: Компьютер. сеть Науч. б-ки Перм. нац. исслед. политехн. ун-та, свободный.». </p> <p>Раздел 8.2 «Компьютерные обучающие и контролирующие программы» считать раздел 8.3 и наименование изложить в следующей редакции: «Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине».</p> <p>Раздел 8.3 «Программные инструментальные средства» считать раздел 8.4 «Перечень программного обеспечения, в том числе компьютерные обучающие и контролирующие программы».</p> <p>Раздел 8.4 «Аудио- и видео-пособия» считать разделом 8.5.</p> <p>Наименование раздела 9 изложить в следующей редакции: «Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине».</p>	
2.		
3.		
4.		
5.		