

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



**Пермский национальный исследовательский  
политехнический университет**

Электротехнический факультет  
Кафедра автоматики и телемеханики



**УТВЕРЖДАЮ**

Проректор по учебной работе  
д-р техн. наук, проф.

*Н. В. Лобов*  
Н. В. Лобов  
2014 г.

**УНИФИЦИРОВАННЫЙ УЧЕБНО-МЕТОДИЧЕСКИЙ КОМПЛЕКС  
ДИСЦИПЛИНЫ**

**«Организационное и правовое обеспечение информационной безопасности»**

**РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ**

Основная образовательная программа подготовки бакалавров и специалистов  
по направлению: 090900.62 «Информационная безопасность»  
по специальности: 090303.65 «Информационная безопасность автоматизиро-  
ванных систем»

<b>Профиль подготовки бакалавра</b>	- 09090003.62 Комплексная защита объектов информа- тизации
<b>Специализация специалиста</b>	- 09030307.65 Обеспечение информационной безопас- ности распределенных информационных систем
<b>Квалификация (степень) выпускника</b>	- бакалавр/ специалист
<b>Специальное звание выпускника</b>	- специалист по защите информации
<b>Выпускающая кафедра</b>	«Автоматика и телемеханика»
<b>Форма обучения</b>	очная

**Курс: 3 Семестр: 5,6**

**Трудоёмкость:**

Кредитов по рабочему учебному плану:	8	ЗЕТ
Часов по рабочему учебному плану:	288	АЧ

**Виды контроля:**

Экзамен: 5,6

Пермь 2014 г.

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» января 2017 г. № 18

**УЧЕБНО-МЕТОДИЧЕСКИЙ КОМПЛЕКС ДИСЦИПЛИНЫ**  
**«Организационное и правовое обеспечение информационной безопасности»**  
**РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ**

**Направление подготовки:** 10.03.01 Информационная безопасность,  
**Направленность (профиль)**  
**образовательной программы:** Комплексная защита объектов информатизации

**Специальность:** 10.05.03 Информационная безопасность автоматизи-  
рованных систем

**Специализация:** Обеспечение информационной безопасности распре-  
деленных информационных систем

**Квалификация выпускника:** бакалавр, специалист

**Выпускающая кафедра:** Автоматика и телемеханика

**Форма обучения:** очная

**Курс:** 3      **Семестр:** 5,6

**Трудоемкость:**

Кредитов по рабочему учебному плану (БУП):

8

Часов по рабочему учебному плану (БУП):

288

**Виды контроля:**

Экзамен: - 5,6

Зачет: - нет

Курсовой проект: - нет

Курсовая работа: - нет

Пермь 2017 г.

**Рабочая программа дисциплины «Организационное и правовое обеспечение информационной безопасности» разработана на основании:**

- федерального государственного образовательного стандарта высшего профессионального образования утвержденного приказом Министерства образования и науки Российской Федерации «17» января 2011 г. № 60, по направлению подготовки (специальности) 090303 «Информационная безопасность автоматизированных систем» [квалификация (степень) «специалист»];
- федерального государственного образовательного стандарта высшего профессионального образования, утвержденного приказом Министерством образования и науки Российской Федерации от «28» октября 2009 г., № 496, по направлению подготовки 090900 Информационная безопасность [квалификация (степень) «бакалавр»];
- компетентностной модели (КМ) выпускника ООП по профилю подготовки 090900.03.62 - Информационная безопасность, утвержденной «05» февраля 2011 г.;
- компетентностной модели (КМ) выпускника ООП по специализации подготовки 090303.07.65 - Обеспечение информационной безопасности распределенных информационных систем, утвержденной «05» февраля 2011 г.;
- рабочего учебного плана очной формы обучения по профилю подготовки 090900.03.62 - Информационная безопасность, (набор 2011 года), утвержденного «07» июня 2011 г.
- рабочего учебного плана очной формы обучения по специализации подготовки 090303.07.65 - Обеспечение информационной безопасности распределенных информационных систем, (набор 2011 года), утвержденного «29» августа 2011 г.

**Рабочая программа согласована с рабочей программой дисциплин:** «Введение в специальность», «Основы информационной безопасности», «Комплексная система защиты информации на предприятии», «Управление информационной безопасностью».

Разработчик: к.т.н.

  
\_\_\_\_\_ А.С. Шабуров

Рецензент: к.т.н., профессор

  
\_\_\_\_\_ А.Н. Данилов

**Рабочая программа рассмотрена и одобрена на заседании кафедры «Автоматика и телемеханика» «26» марта 2013 г., протокол № 26.**

Заведующий выпускающей  
кафедрой «Автоматика и телемеханика»,  
д.т.н., профессор

  
\_\_\_\_\_ А.А.Южаков

**Рабочая программа рассмотрена и одобрена учебно-методической комиссией электротехнического факультета «5» мая 2013 г., протокол № 5.**

Председатель учебно-методической комиссии  
электротехнического факультета,  
к.т.н., профессор

  
\_\_\_\_\_ А. Л. Гольдштейн

СОГЛАСОВАНО

Начальник управления образовательных программ, к.т.н., доцент

  
\_\_\_\_\_ Д. С. Репецкий

**Рабочая программа дисциплины «Организационное и правовое обеспечение информационной безопасности» разработана на основании:**

- Федерального государственного образовательного стандарта высшего образования по направлению подготовки 10.03.01 Информационная безопасность (уровень бакалавриата), утвержденного приказом Министерства образования и науки Российской Федерации от «01» декабря 2016 г. № 1515;
- 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 бакалавриата по направлению подготовки 10.03.01 Информационная безопасность направленности (профиля) «Комплексная защита объектов информатизации», утвержденной «24» июня 2013 г. (с изменениями, в связи с переходом на ФГОС ВО);
- 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 бакалавриата по направлению подготовки 10.03.01 Информационная безопасность, направленности (профиля) «Комплексная защита объектов информатизации», утвержденного «22» декабря 2016 г.
- 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:

Правоведение, Основы управленческой деятельности, Документоведение, Социология и политология, Основы предпринимательской деятельности, Основы построения инфокоммуникационных систем и сетей, Защита и обработка конфиденциальных документов базового учебного плана образовательной программы высшего образования - программы бакалавриата по направлению 10.03.01 Информационная безопасность, направленности (профиля) Комплексная защита объектов информатизации;

Правоведение, Основы управленческой деятельности, Социология и политология, Основы построения инфокоммуникационных систем и сетей, Защита и обработка конфиденциальных документов базового учебного плана образовательной программы высшего образования - программы по специальности 10.05.03 Информационная безопасность автоматизированных систем, специализации Обеспечение информационной безопасности распределенных информационных систем.

## 1. Общие положения

**1.1. Цель дисциплины** - освоение дисциплинарных компетенций по применению комплекса мероприятий в системе защиты информации на основе реализации требований по правовой защите информации и организационному обеспечению информационной безопасности.

В процессе изучения дисциплины студент осваивает части следующих компетенций по направлениям подготовки ВПО:

Таблица 1.1 Заданные ФГОС ВПО общекультурные и профессиональные компетенции по направлению подготовки / специальности

№	Код направления/специальности	Наименование направления/специальности	Компетенции, формируемые на основе базовых учебных планов	
			Код компетенции	Формулировка компетенции
1.	090900.62	Информационная безопасность	ОК-1	способность осознавать необходимость соблюдения Конституции Российской Федерации, прав и обязанностей гражданина своей страны, гражданского долга и проявления патриотизма
			ОК-5	способность к кооперации с коллегами, работе в коллективе
			ПК-4	способность формировать комплекс мер по информационной безопасности с учетом его правовой обоснованности, административно-управленческой и технической реализуемости и экономической целесообразности
2.	090303.65	Информационная безопасность автоматизированных систем	ОК-1	способность действовать в соответствии с Конституцией Российской Федерации, исполнять свой гражданский и профессиональный долг, руководствуясь принципами законности и патриотизма
			ОК-6	способность к работе в коллективе, кооперации с коллегами, способность в качестве руководителя подразделения, лидера группы сотрудников формировать цели команды, принимать организационно-управленческие решения в нестандартных ситуациях и нести за них ответственность, предупреждать и конструктивно разрешать конфликтные ситуации в процессе профессиональной деятельности
			ПК-6	способность использовать нормативные правовые акты в своей профессиональной деятельности

В целях унификации на основании базовых компетенций выпускника, определенных ФГОС ВПО по направлениям подготовки, разработаны следующие унифицированные общекультурные компетенции (УОК) и унифицированные профессиональные компетенции (УПК)

**Унифицированная общекультурная компетенция (УОК-1)**

*Способность осознанно действовать в соответствии с Конституцией Российской Федерации, исполнять свой гражданский и профессиональный долг, руководствуясь принципами законности и патриотизма*

**Унифицированная общекультурная компетенция (УОК-2)**

*Способность к работе в коллективе, кооперации с коллегами, в качестве руководителя подразделения, лидера группы сотрудников, формированию цели команды, принимать организационно-управленческие решения в нестандартных ситуациях и нести за них ответственность, предупреждать и конструктивно разрешать конфликтные ситуации в процессе профессиональной деятельности*

**Унифицированная профессиональная компетенция (УПК-1)**

*Способность использовать нормативные правовые акты в своей профессиональной деятельности, формировать комплекс мер по информационной безопасности с учетом его правовой обоснованности, административно-управленческой и технической реализуемости и экономической целесообразности*

Таблица 1.2 Обоснование разработки унифицированных компетенций

№	Направление подготовки		Соответствие унифицированной компетенции и базовой компетенции ФГОС ВПО		
	Код	Наименование			
			Способность осознанно действовать в соответствии с Конституцией Российской Федерации, исполнять свой гражданский и профессиональный долг, руководствуясь принципами законности и патриотизма (УОК-1)	Способность к работе в коллективе, кооперации с коллегами, в качестве руководителя подразделения, лидера группы сотрудников, формированию цели команды, принимать организационно-управленческие решения в нестандартных ситуациях и нести за них ответственность, предупреждать и конструктивно разрешать конфликтные ситуации в процессе профессиональной деятельности (УОК-2)	Способность использовать нормативные правовые акты в своей профессиональной деятельности, формировать комплекс мер по информационной безопасности с учетом его правовой обоснованности, административно-управленческой и технической реализуемости и экономической целесообразности (УПК-1)

1	2	3	4	5	6
1.	090900.62	Информационная безопасность	способность осознать необходимость соблюдения Конституции Российской Федерации, прав и обязанностей гражданина своей страны, гражданского долга и проявления патриотизма (ОК-1)	способность к кооперации с коллегами, работе в коллективе (ОК-5)	способность формировать комплекс мер по информационной безопасности с учетом его правовой обоснованности, административно-управленческой и технической реализуемости и экономической целесообразности (ПК-4)
2.	090303.65	Информационная безопасность автоматизированных систем	способность действовать в соответствии с Конституцией Российской Федерации, исполнять свой гражданский и профессиональный долг, руководствуясь принципами законности и патриотизма (ОК-1)	способность к работе в коллективе, кооперации с коллегами, способность в качестве руководителя подразделения, лидера группы сотрудников формировать цели команды, принимать организационно-управленческие решения в нестандартных ситуациях и нести за них ответственность, предупреждать и конструктивно разрешать конфликтные ситуации в процессе профессиональной деятельности (ОК-6)	способность использовать нормативные правовые акты в своей профессиональной деятельности (ПК-6)

## 1.2. Задачи дисциплины:

- изучение основных положений, понятий и категорий международных правовых документов Конституции и нормативно-правовых актов Российской Федерации в области обеспечения информационной безопасности;
- изучение правовых основ и принципов организации защиты государственной тайны и конфиденциальной информации, задач органов защиты государственной тайны и служб защиты информации на предприятиях;
- изучение организации работы и нормативных правовых актов и стандартов по лицензированию деятельности в области обеспечения защиты государственной тайны, технической защиты конфиденциальной информации, по аттестации объектов информатизации и сертификации средств защиты информации;
- приобретение умений в разработке проектов нормативных и организационно-распорядительных документов в области обеспечения информационной безопасности и их

применении;

– приобретение навыков работы в организации и обеспечении режима секретности, физической защиты объектов, методах организации работы с персоналом и управлению деятельностью служб защиты информации на предприятии.

После изучения дисциплины обучающийся должен демонстрировать следующие результаты:

***знать:***

– основы российской правовой системы и законодательства, правового статуса личности, организации деятельности органов государственной власти Российской Федерации по защите информации;

– характеристику основных отраслей российского права, правовые основы обеспечения национальной безопасности РФ;

– виды и степень ответственности за правонарушения и преступления в информационной сфере;

– порядок работы с персоналом по вопросам обеспечения защиты информации ограниченного доступа, проведения мероприятий по физической и технической защите конфиденциальной информации, организации службы безопасности предприятия;

– основы организационного и правового обеспечения информационной безопасности, основные нормативные правовые акты в области обеспечения информационной безопасности и нормативные методические документы ФСБ России и ФСТЭК России в области защиты информации;

– правовые основы организации защиты государственной тайны и конфиденциальной информации, задачи органов защиты государственной тайны и служб защиты информации на предприятиях;

***уметь:***

– определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите;

– анализировать правовые акты и осуществлять правовую оценку информации;

– предпринимать необходимые меры по восстановлению нарушенных прав;

– организовывать работы по проверке кандидатов на должность, текущую работу с персоналом по обеспечению информационной безопасности;

– разрабатывать проекты нормативных и организационно-распорядительных документов, регламентирующих работу по защите информации;

– применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности;

***владеть:***

– навыками поиска нормативной правовой информации, необходимой для профессиональной деятельности навыками работы с нормативными правовыми актами;

– навыками работы с персоналом, принятия организационно-управленческих решений, в том числе в нестандартных ситуациях в целях обеспечения информационной безопасности;

– навыками организации охраны объектов информатизации и обеспечения режима секретности, организации и управления деятельностью службы защиты информации на предприятии.



### 1.3. Предметом освоения дисциплины являются следующие объекты:

- методы правовой защиты информации;
- правовые основы защиты государственной, коммерческой, служебной, профессиональной тайны, персональных данных;
- правовая основа и порядок допуска и доступа к информации ограниченного доступа;
- система правовой ответственности за правонарушения в информационной сфере;
- правовые основы деятельности подразделений защиты информации;
- порядок и принципы засекречивания и рассекречивания информации;
- порядок организации охраны объектов информатизации, внутриобъектового и пропускного режима;
- организация работы с персоналом по вопросам защиты информации;
- организация подготовки и проведения совещаний и заседаний по конфиденциальным вопросам,
- организация защиты информации в публикаторской и рекламной деятельности;
- организация деятельности службы безопасности предприятия.

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

Дисциплина «Организационное и правовое обеспечение информационной безопасности» относится к базовой части цикла профессиональных дисциплин по направлению 090900 Информационная безопасность (квалификация (степень) «бакалавр») и специальности 090303 Информационная безопасность автоматизированных систем (квалификация (степень) «специалист»).

Дисциплина является обязательной при освоении ООП ВПО по указанному направлению и подготовки по специальности.

В таблице 1.3 приведены предшествующие и последующие дисциплины, направленные на формирование компетенций, заявленных в пункте 1.1.

Таблица 1.1 - Дисциплины, направленные на формирование компетенций

Направление (специальность)	Код компетенции	Наименование компетенций	Предшествующие дисциплины	Последующие дисциплины
090900.62	ОК-1	Способность осознавать необходимость соблюдения Конституции Российской Федерации, прав и обязанностей гражданина своей страны, гражданского долга и проявления патриотизма	Правоведение Социология и политология	Управление информационной безопасностью
	ОК-5	Способность к кооперации с коллегами, работе в коллективе	Социология и политология	Управление информационной безопасностью
	ПК-4	Способность формировать	Правоведение	Комплексная за-

		комплекс мер по информационной безопасности с учетом его правовой обоснованности, административно-управленческой и технической реализуемости и экономической целесообразности		щита информации на предприятии
090303.65	ОК-1	Способность действовать в соответствии с Конституцией Российской Федерации, исполнять свой гражданский и профессиональный долг, руководствуясь принципами законности и патриотизма	Правоведение Социология и политология	Информационная безопасность в экономике
	ОК-6	Способность к работе в коллективе, кооперации с коллегами, в качестве руководителя подразделения, лидера группы сотрудников формировать цели команды, принимать организационно-управленческие решения в нестандартных ситуациях и нести за них ответственность, предупреждать и конструктивно разрешать конфликтные ситуации в процессе профессиональной деятельности	Экономика Основы управленческой деятельности Социология и политология Основы предпринимательской деятельности	Управление информационной безопасностью
	ПК-6	Способность использовать нормативные правовые акты в своей профессиональной деятельности	Правоведение	Основы построения информационных систем и сетей Защита и обработка конфиденциальных документов Информационная безопасность в банковской системе

## 2. Требования к результатам освоения учебной дисциплины

Дисциплина обеспечивает формирование части компетенции УОК-1, УОК-2 и УПК-1:

### 2.1. Дисциплинарная карта компетенции УОК-1

Код УОК-1	<b>Формулировка унифицированной дисциплинарной компетенции</b> Способность осознанно действовать в соответствии с Конституцией Российской Федерации, исполнять свой гражданский и профессиональный долг, руководствуясь принципами законности и патриотизма
--------------	--

### Требования к компонентному составу компетенции

Перечень компонентов	Виды учебной работы	Средства оценки
<b>Знает:</b> <ul style="list-style-type: none"> <li>– основы российской правовой системы и законодательства, правового статуса личности, организации деятельности органов государственной власти Российской Федерации по защите информации;</li> <li>– характеристику основных отраслей российского права, правовые основы обеспечения национальной безопасности РФ;</li> </ul>	Лекции Семинарские занятия Самостоятельная работа студентов по изучению теоретического материала	Вопросы для текущего и рубежного контроля
<b>Умеет:</b> <ul style="list-style-type: none"> <li>– определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите;</li> <li>– анализировать правовые акты и осуществлять правовую оценку информации;</li> </ul>	Практические занятия Самостоятельная работа студентов по решению практических задач Самостоятельная работа студентов по подготовке к экзамену	Отчет за выполнение практических заданий на ПЗ Отчёт по индивидуальным заданиям по модулю
<b>Владеет:</b> <ul style="list-style-type: none"> <li>– навыками поиска нормативной правовой информации, необходимой для профессиональной деятельности навыками работы с нормативными правовыми актами</li> </ul>	Самостоятельная работа студентов по решению практических задач Самостоятельная работа по подготовке к экзамену	Отчет за выполнение практических заданий на ПЗ Отчёт по индивидуальным заданиям по модулю

## 2.1. Дисциплинарная карта компетенции УОК-2

Код УОК-2	<p><b>Формулировка унифицированной дисциплинарной компетенции</b></p> <p>Способность к работе в коллективе, кооперации с коллегами, в качестве руководителя подразделения, лидера группы сотрудников, формированию цели команды, принимать организационно-управленческие решения в нестандартных ситуациях и нести за них ответственность, предупреждать и конструктивно разрешать конфликтные ситуации в процессе профессиональной деятельности</p>
--------------	--

### Требования к компонентному составу компетенции

Перечень компонентов	Виды учебной работы	Средства оценки
<p><b>Знает:</b></p> <ul style="list-style-type: none"> <li>– виды и степень ответственности за правонарушения и преступления в информационной сфере;</li> <li>– порядок работы с персоналом по вопросам обеспечения защиты информации ограниченного доступа, проведения мероприятий по физической и технической защите конфиденциальной информации, организации службы безопасности предприятия;</li> </ul>	<p>Лекции</p> <p>Семинарские занятия</p> <p>Самостоятельная работа студентов по изучению теоретического материала</p>	<p>Вопросы для текущего и рубежного контроля</p>
<p><b>Умеет:</b></p> <ul style="list-style-type: none"> <li>– предпринимать необходимые меры по восстановлению нарушенных прав;</li> <li>– организовывать работы по проверке кандидатов на должность, текущую работу с персоналом по обеспечению информационной безопасности;</li> </ul>	<p>Практические занятия</p> <p>Самостоятельная работа студентов по решению практических задач</p> <p>Самостоятельная работа студентов по подготовке к экзамену</p>	<p>Отчет за выполнение практических заданий на ПЗ</p> <p>Отчёт по индивидуальным заданиям по модулю</p>
<p><b>Владет:</b></p> <ul style="list-style-type: none"> <li>– навыками работы с персоналом, принятия организационно-управленческих решений, в том числе в нестандартных ситуациях в целях обеспечения информационной безопасности;</li> </ul>	<p>Самостоятельная работа студентов по решению практических задач</p> <p>Самостоятельная работа по подготовке к экзамену</p>	<p>Отчет за выполнение практических заданий на ПЗ</p> <p>Отчёт по индивидуальным заданиям по модулю</p>

## 2.2. Дисциплинарная карта компетенции УПК-1

Код УПК-1	<p><b>Формулировка унифицированной дисциплинарной компетенции</b></p> <p>Способность использовать нормативные правовые акты в своей профессиональной деятельности, формировать комплекс мер по информационной безопасности с учетом его правовой обоснованности, административно-управленческой и технической реализуемости и экономической целесообразности</p>
--------------	--

### Требования к компонентному составу компетенции

Перечень компонентов	Виды учебной работы	Средства оценки
<p><b>Знает:</b></p> <ul style="list-style-type: none"> <li>– основы организационного и правового обеспечения информационной безопасности, основные нормативные правовые акты в области обеспечения информационной безопасности и нормативные методические документы ФСБ России и ФСТЭК России в области защиты информации;</li> <li>– правовые основы организации защиты государственной тайны и конфиденциальной информации, задачи органов защиты государственной тайны и служб защиты информации на предприятиях;</li> </ul>	<p>Лекции Семинарские занятия Самостоятельная работа студентов по изучению теоретического материала</p>	<p>Вопросы для текущего и рубежного контроля</p>
<p><b>Умеет:</b></p> <ul style="list-style-type: none"> <li>– разрабатывать проекты нормативных и организационно-распорядительных документов, регламентирующих работу по защите информации;</li> <li>– применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности;</li> </ul>	<p>Практические занятия Самостоятельная работа студентов по решению практических задач Самостоятельная работа студентов по подготовке к экзамену</p>	<p>Отчет за выполнение практических заданий на ПЗ Отчёт по индивидуальным заданиям по модулю</p>
<p><b>Владет:</b></p> <ul style="list-style-type: none"> <li>– навыками организации охраны объектов информатизации и обеспечения режима секретности, организации и управления деятельностью службы защиты информации на предприятии;</li> </ul>	<p>Самостоятельная работа студентов по решению практических задач Самостоятельная работа по подготовке к экзамену</p>	<p>Отчет за выполнение практических заданий на ПЗ Отчёт по индивидуальным заданиям по модулю</p>

### 3. Объем дисциплины и виды учебной работы

3.1. 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 (ЛК);
- 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 – Объём и виды учебной работы

№ п/п	Виды учебной работы	Трудоемкость в АЧ			Форма представления результатов
		5	6	Всего	
1	2	3	4	5	6
1	<b>Аудиторная работа:</b>	<b>54</b>	<b>48</b>	<b>102</b>	
	– в том числе в интерактивной форме	14	14	28	
	– лекции (Л)	24	22	46	конспект лекций
	– в том числе в интерактивной форме	4	4	8	
	– практические занятия (ПЗ), семинарские занятия (СЗ)	28	24	52	отчет о выполнении
	– в том числе в интерактивной форме	10	10	20	
2	Контроль самостоятельной работы (КСР)	2	2	4	
3	<b>Самостоятельная работа студентов (СРС)</b>	<b>54</b>	<b>60</b>	<b>114</b>	
	Самостоятельное изучение теоретического материала (ИТМ)	24	30	54	отчет по вопросам для текущего и рубежного контроля
	Выполнение индивидуальных заданий по модулю (ИЗМ)	30	30	60	отчёт о выполнении
4	Итоговая аттестация по дисциплине:	36	36	72	<b>Экзамен</b>
3	<b>Трудоемкость дисциплины, всего:</b>	<b>144</b>	<b>144</b>	<b>288</b>	
	<b>в часах (АЧ)</b> <b>в зачетных единицах (ЗЕТ)</b>	<b>4</b>	<b>4</b>	<b>8</b>	

## 4. Содержание учебной дисциплины

### 4.1. Модульный тематический план

Общая структура содержания дисциплины представлена тематическим планом, который задает распределение трудоемкостей модулей, разделов и тем содержания по видам аудиторной и самостоятельной работы (табл.4.1).

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.	Трудоемкость 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	1.1	4	2	2		2	2				6
		1.2	4	2	2		2	2				6
		1.3	4	2	2		12	2	10			16
	<b>Всего по модулю:</b>		<b>12</b>	<b>6</b>	<b>6</b>		<b>16</b>	<b>6</b>	<b>10</b>			<b>28</b>
2	1	1.4	4	2	2		2	2				6
		1.5	6	2	4		2	2				8
		1.6	6	2	4		4	4				10
	1.7	6	4	2		14	4	10			20	
<b>Всего по модулю:</b>		<b>22</b>	<b>10</b>	<b>12</b>		<b>22</b>	<b>12</b>	<b>10</b>			<b>44</b>	
3	1	1.8	4	2	2		2	2				6
		1.9	8	2	4	2	2	2				10
		1.10	8	4	4		12	2	10			20
	<b>Всего по модулю:</b>		<b>20</b>	<b>8</b>	<b>10</b>	<b>2</b>	<b>16</b>	<b>6</b>	<b>10</b>			<b>36</b>
<b>Всего по разделу:</b>			<b>54</b>	<b>24</b>	<b>28</b>	<b>2</b>	<b>54</b>	<b>24</b>	<b>30</b>			<b>108</b>
4	2	2.1	4	2	2		2	2				6
		2.2	4	2	2		2	2				6
		2.3	4	2	2		12	2	10			16
	<b>Всего по модулю:</b>		<b>12</b>	<b>6</b>	<b>6</b>		<b>16</b>	<b>6</b>	<b>10</b>			<b>28</b>
5	2	2.4	4	2	2		2	2				6
		2.5	4	2	2		4	4				8
		2.6	8	4	4		14	4	10			22
	<b>Всего по модулю:</b>		<b>16</b>	<b>8</b>	<b>8</b>		<b>20</b>	<b>10</b>	<b>10</b>			<b>36</b>
6	2	2.7	4	2	2		2	2				6
		2.8	4	2	2		4	4				8
		2.9	8	2	4	2	4	4				12
	2.10	4	2	2		14	4	10			28	
<b>Всего по модулю:</b>		<b>20</b>	<b>8</b>	<b>10</b>	<b>2</b>	<b>24</b>	<b>14</b>	<b>10</b>			<b>44</b>	
<b>Всего по разделу:</b>			<b>48</b>	<b>22</b>	<b>24</b>	<b>2</b>	<b>60</b>	<b>30</b>	<b>30</b>			<b>108</b>
Итоговая аттестация										72	72	
Итого			<b>102</b>	<b>46</b>	<b>52</b>	<b>4</b>	<b>114</b>	<b>54</b>	<b>60</b>	<b>72</b>	<b>288/8</b>	

## 4.2. Содержание разделов и тем учебной дисциплины

### Раздел I. Правовое обеспечение информационной безопасности

**Модуль 1. Информационные отношения и правовой режим защиты информации ограниченного доступа** АРС: Л - 6 ч.; ПЗ (СЗ) - 6 ч., СРС: ИТМ - 6 ч., ИЗМ (ИЗМ-1) - 10 ч.

**Тема 1.1 Информационные отношения как объект правового регулирования. Законодательство Российской Федерации в области информационной безопасности.** Структура информационной сферы и характеристика ее элементов. Информация как объект правоотношений. Категории информации по условиям доступа к ней и распространения. Конституционные гарантии прав граждан в информационной сфере и механизм их реализации. Субъекты и объекты правоотношений в области информационной безопасности. Система нормативных правовых актов, регулирующие обеспечение информационной безопасности в Российской Федерации Понятие и виды информации ограниченного доступа по законодательству РФ.

**Тема 1.2. Правовой режим защиты государственной тайны.** Понятие правового режима защиты государственной тайны. Система нормативных правовых актов, регламентирующих обеспечение сохранности сведений, составляющих государственную тайну в Российской Федерации. Государственная тайна как особый вид защищаемой информации и ее характерные признаки. Принципы и механизмы отнесения сведений к государственной тайне, их засекречивания и рассекречивания.

**Тема 1.3. Правовой режим защиты информации конфиденциального характера.** Понятие информации конфиденциального характера по российскому законодательству. Основные виды конфиденциальной информации: персональные данные, служебная тайна, коммерческая тайна, банковская тайна, профессиональная тайна, тайна следствия и судопроизводства. Правовой режим конфиденциальной информации: содержание и особенности. Основные требования, предъявляемые к организации защиты конфиденциальной информации.

**Модуль 2. Правовая защита различных видов конфиденциальной информации** АРС: Л - 10 ч.; ПЗ (СЗ) - 12 ч., СРС: ИТМ - 12 ч., ИЗМ (ИЗМ-2) - 10 ч.

**Тема 1.4. Институт правовой защиты служебной тайны.** Правовые основы защиты служебной тайны. Нормативно-правовые акты, регулирующие правовую защиту служебной тайны. Защита в режиме служебной тайны сведений, доступ к которым ограничивается в соответствии с законодательством, при обращении и хранении таких сведений (информации) в органах государственной власти и органах местного самоуправления. Защита служебной тайны в соответствии с «Положением о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти».

**Тема 1.5. Институт правовой защиты коммерческой тайны.** Правовые основы защиты коммерческой тайны. Источники права о коммерческой тайне. Объекты и субъекты права на коммерческую тайну. Права и обязанности обладателя коммерческой тайны. Порядок установления режима коммерческой тайны при заключении и выполнении гражданско-правовых договоров. Юридическая защита права на коммерческую тайну. Ответственность за нарушение прав на коммерческую тайну.

**Тема 1.6. Институт правовой защиты банковской тайны.** Правовые основы защиты банковской тайны. Источники права о банковской тайне. Объекты и субъекты права на банковскую тайну. Права владельца банковской тайны в отношении сведений, составляющих



его банковскую тайну. Обязанности пользователей банковской тайны.

**Тема 1.7. Институт правовой защиты профессиональной тайны.** Понятие профессиональной тайны. Правовые основы защиты профессиональной тайны. Источники права о профессиональной тайне. Объекты и субъекты права на профессиональную тайну. Критерии охраноспособности права на профессиональную тайну. Права доверителя в отношении сведений, ставших на законных основаниях известными держателю профессиональной тайны. Особенности правовой защиты различных субинститутов профессиональной тайны

**Модуль 3. Защита персональных данных и государственное регулирование деятельности по защите информации** АРС: Л - 8 ч; ПЗ (СЗ) - 10 ч., СРС:- ИТМ - 6 ч., ИЗМ (ИЗМ-3) - 10 ч.

**Тема 1.8. Институт правовой защиты персональных данных.** Правовые основы защиты информации персонального характера. Закон РФ «О персональных данных», подзаконные нормативно-правовые документы о порядке правовой защиты персональных данных. Государственный надзор и контроль обработки персональных данных.

**Тема 1.9. Государственное регулирование деятельности в области защиты информации.** Понятие лицензирования по российскому законодательству. Виды деятельности, подлежащие лицензированию. Правовая регламентация лицензионной деятельности в области обеспечения информационной безопасности. Объекты лицензирования и участники лицензионных отношений в сфере защиты информации. Органы лицензирования и их полномочия. Организация лицензирования в сфере обеспечения информационной безопасности. Контроль за соблюдением лицензиатами условий ведения деятельности. Правовые основы сертификации в области защиты информации.

**Тема 1.10. Правонарушения в информационной сфере и особенности защиты от них.** Особенности правонарушений в информационной сфере. Преступления в сфере компьютерной информации: виды, состав. Основы расследования преступлений в сфере компьютерной информации. Правовая защита информационных систем. Правовая защита результатов интеллектуальной деятельности.

## **Раздел II. Организационное обеспечение информационной безопасности**

**Модуль 4.** Основные понятия и организация защиты государственной тайны. АРС: Л - 6 ч; ПЗ (СЗ) - 6 ч., СРС: ИТМ - 6 ч., ИЗМ (ИЗМ-4) - 10 ч.

**Тема 2.1. Понятие организационной защиты информации.** Введение в организационное обеспечение информационной безопасности. Список рекомендованной литературы. Сущность организационных методов защиты информации. Соотношение организационных мер защиты информации с мерами правового и технического характера. Основные термины, связанные с организацией защиты информации.

**Тема 2.2. Организация режима секретности.** Организационные меры, направленные на защиту государственной тайны. Режим секретности как основной порядок деятельности в сфере защиты государственной тайны. Особенности системы организационной защиты государственной тайны. Распределение между уровнями государственного управления полномочий, управленческих функций и задач по защите государственной тайны. Организация деятельности режимно-секретных органов. Установление и изменение степени секретности сведений, отнесенных к государственной тайне. Понятие «рассекречивание сведений». Основания для рассекречивания сведений.

**Тема 2.3. Допуск к государственной тайне.** Порядок допуска и доступа к государственной тайне. Основные принципы допускной работы. Номенклатура должностей работников, подлежащих оформлению на допуск и порядок ее составления и утверждения. Документальное оформление для отправки на согласование. Процедура оформления и переоформления допусков и ее документирование, подлежащее согласованию с органами государственной безопасности. Организация доступа к сведениям, составляющим государственную тайну.

**Модуль 5. Организация охраны, режима и работы с персоналом.** АРС: Л - 8 ч; ПЗ (СЗ) - 8 ч., СРС: ИТМ - 10 ч., ИЗМ (ИЗМ-5) - 10 ч.

**Тема 2.4. Организация охраны объектов.** Понятие «охрана». Цели и задачи охраны. Объекты охраны: территория, здания, помещения, персонал, информационные ресурсы, материальные и финансовые ценности. Особенности их охраны. Виды, способы и особенности охраны различных объектов. Понятие о рубежах охраны. Многорубежная система охраны. Факторы выбора методов и средств охраны. Организация охраны объектов защиты в процессе их транспортировки.

**Тема 2.5. Организация режимных мероприятий.** Понятие «режим», цели и задачи режимных мероприятий. Виды режима. Организация пропускного режима. Основные положения инструкции об организации пропускного режима и работе бюро пропусков. Виды пропускных документов. Порядок организации работы бюро пропусков. Контрольно-пропускные пункты, их оборудование и организация работы. Понятие «внутриобъектовый режим» и его общие требования. Противопожарный режим и его обеспечение.

**Тема 2.6. Текущая работа с персоналом, обладающим конфиденциальной информацией.** Подбор и расстановка кадров. Направления и методы работы с персоналом, обладающим конфиденциальной информацией. Организация обучения персонала. Основные формы обучения и методы контроля знаний. Мотивация персонала к выполнению требований по защите информации. Основные формы воздействия на персонал как методы мотивации: вознаграждение, управление карьерой, профессиональная этика. Организация контроля соблюдения персоналом требований режима защиты информации. Методы проверки персонала. Организация служебного расследования по фактам разглашения персоналом конфиденциальной информации. Организационные меры по защите информации при увольнении сотрудника.

**Модуль 6. Организация защиты информации в различных направлениях деятельности предприятия (организации).** АРС: Л - 8 ч; ПЗ (СЗ) - 10 ч., СРС: ИТМ - 14 ч., ИЗМ (ИЗМ-6) - 10 ч.

**Тема 2.7. Организация подготовки и проведения конфиденциальных переговоров.** Основные требования, предъявляемые к подготовке и проведению конфиденциальных переговоров. Основные этапы проведения конфиденциальных переговоров. Подготовка помещения для проведения конфиденциальных переговоров. Подготовка программы проведения конфиденциальных переговоров. Порядок встречи и регистрации приглашенных лиц. Порядок проведения конфиденциальных переговоров.

**Тема 2.8. Организация защиты информации при приеме в организации посетителей, командированных лиц, иностранных представителей.** Требования режима защиты информации при приеме в организации посетителей. Порядок доступа посетителей и командированных лиц к конфиденциальной информации. Порядок пребывания посетителей на территории и в помещениях организации. Требования к программе приема иностранных представителей. Основные положения плана мероприятий по обеспечению режима конфи-

денциальности в период пребывания иностранных представителей на объекте. Организация работы с иностранными представителями. Требования к помещениям, в которых проводится прием иностранных представителей. Обеспечение защиты информации при выезде за рубеж командированных лиц.

**Тема 2.9. Защита информации в рекламной деятельности, при подготовке материалов к открытому опубликованию.** Основные виды и формы рекламы. Общие требования режима защиты информации в процессе рекламной деятельности. Основные методы защиты информации в рекламной деятельности. Понятие «публикация в открытой печати». Общие требования режима защиты конфиденциальной информации при опубликовании материалов в открытой печати. Особенности защиты информации при опубликовании материалов, определяемые характером деятельности организации, целями публикации, содержанием и характером публикации.

**Тема 2.10. Организация работы службы безопасности предприятия.** Концепция безопасности предприятия (организации) и ее содержание. Политика информационной безопасности. Подразделения, обеспечивающие ИБ предприятия: основные функции, содержание деятельности, структура, обязанности сотрудников. Варианты организационных структур, обеспечивающих защиту информации. Основные документы службы информационной безопасности.

#### 4.3 Перечень тем практических занятий (семинаров)

Таблица 4.2 – Темы семинарских (СЗ), практических занятий (ПЗ)

№ п/п	Номер темы дисциплины	Наименование темы практического занятия
1	1.1	Информационные отношения как объект правового регулирования
2	1.2	Правовой режим защиты государственной тайны
3	1.3	Правовой режим защиты информации конфиденциального характера
4	1.4	Институт правовой защиты служебной тайны
5	1.5	Институт правовой защиты коммерческой тайны
6	1.6	Институт правовой защиты банковской тайны
7	1.7	Институт правовой защиты профессиональной тайны
8	1.8	Институт правовой защиты персональных данных
9	1.9	Государственное регулирование деятельности в области защиты информации (ПЗ)
10	1.10	Преступления в сфере компьютерной информации
11	2.1	Понятие и сущность организационной защиты информации
12	2.2	Организация режима секретности
13	2.3	Допуск к государственной тайне
14	2.4	Организация многорубежной системы охраны (ПЗ)
15	2.5	Организация режимных мероприятий (ПЗ)
16	2.6	Организация служебного расследования по фактам утраты информации (ПЗ)
17	2.7	Организация подготовки и проведения совещаний и заседаний по конфиденциальным вопросам
18	2.8	Организация защиты информации при приеме в организации посетителей и командированных лиц (ПЗ)

1	2	3
19	2.9	Защита информации при публикаторской и рекламной деятельности
20	2.10	Организация работы службы безопасности предприятия (ПЗ)

#### 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	2	3
1.1	ИТМ: Перспективы развития законодательства в области информационной безопасности	2
1.2	ИТМ: Система контроля за состоянием защиты государственной тайны.	2
1.3	ИТМ: Порядок восстановления нарушенных информационных прав	2
1.3	ИЗМ: В соответствии с перечнем тем для модуля 1, п.п. 4.5.1	10
1.4	ИТМ: Практика совершенствования института сведений ограниченного распространения как основа для формирования и совершенствования института служебной тайны	2
1.5	ИТМ: Права и обязанности органов государственной власти, иных государственных органов и органов местного самоуправления в отношении коммерческой тайны	2
1.6	ИТМ: Защита владельцем банковской тайны своих прав	4
1.7	ИТМ: Обязанности держателя профессиональной тайны. Защита доверителем своих прав	4
1.7	ИЗМ: В соответствии с перечнем тем для модуля 2, п.п. 4.5.1	10
1.8	ИТМ: Возможность использования закона «О частной детективной и охранной деятельности» для правовой защиты персональных данных	2
1.9	ИТМ: Правовая регламентация сертификационной деятельности в области обеспечения информационной безопасности. Органы сертификации и их полномочия	2
1.10	ИТМ: Практика расследования преступлений в сфере компьютерной информации	2
1.10	ИЗМ: В соответствии с перечнем тем для модуля 3, п.п. 4.5.1	10
2.1	ИТМ: Режим защиты информации как составная часть организационной защиты информации	2
2.2	ИТМ: Категорирование объектов для организации защиты государственной тайны	2
2.3	ИТМ: Особенности проведения инструктажа и документального оформления контракта о допуске к государственной тайне	2
2.3	ИЗМ: В соответствии с перечнем тем для модуля 3, п.п. 4.5.1	10

1	2	3
2.4	ИТМ: Безопасность при транспортировке носителей информации. Личная безопасность сотрудников и членов их семей	2
2.5	ИТМ: Средства поиска и досмотра. Обнаружение металлов и взрывчатых веществ	4
2.6	ИТМ: Документирование процедуры увольнения сотрудника	4
2.6	ИЗМ: В соответствии с перечнем тем для модуля 3, п.п. 4.5.1	10
2.7	ИТМ: Порядок реализации режимных мер в ходе проведения выездных конфиденциальных переговоров	2
2.8	ИТМ: Обязанности лиц, участвующих в работе с иностранцами	4
2.9	ИТМ: Порядок выявления каналов утечки информации при организации публикаторской деятельности	4
2.10	ИТМ: Порядок создания и функционирования экспертных комиссий предприятий	4
2.10	ИЗМ: В соответствии с перечнем тем для модуля 3, п.п. 4.5.1	10
	Итого: в ч / в ЗЕ	<b>54/3,17</b>

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

##### **Раздел 1, модули 1,2,3.**

1. Проблемы применения норм права для пресечения компьютерной преступности на международном и внутригосударственном уровне.

2. Области взаимодействия частных охранных предприятий с государственными правоохранительными органами.

3. Правовое обеспечение защиты негосударственных объектов экономики.

4. Состояние и перспективы правовой защиты интеллектуальной собственности в России и за рубежом.

5. Деятельность организаций, выполняющих контролирующие и правоохранительные функции в РФ в области защиты интеллектуальной собственности.

6. Практика применения нормативно-правовой базы лицензирования и сертификации в области защиты государственной тайны в РФ.

7. Практика применения нормативно-правовой базы лицензирования и сертификации в области защиты коммерческой тайны в РФ.

8. Перспективы развития правовой защиты профессиональной тайны.

9. Порядок и регулирование вопросов международного обмена конфиденциальной информацией.

10. Опыт применения российских и международных стандартов безопасности.

11. Правовая защита информационных технологий против компьютерных преступлений.

12. Правовое обеспечение защиты информации в автоматизированных и телекоммуникационных системах.

13. Стандарты безопасности для государственных или коммерческих предприятий, допущенных к сведениям составляющих государственную тайну.

14. Ответственность за совершение компьютерных преступлений как способ правового регулирования отношений в информационной сфере.

15. Правовое регулирование деятельности частных охранных служб в сфере защиты информации.

16. Правовое регулирование защиты персональных данных в России и за рубежом.
17. Правовое регулирование использования специальных технических средств получения и защиты информации.

#### **Раздел 2, модули 4,5,6.**

18. Законодательные акты по вопросам организационного обеспечения информационной безопасности.
19. Соотношение организационных и технических методов защиты информации при использовании технических, в том числе электронных средств передачи, обработки, хранения конфиденциальной информации.
20. Функции высших учебных заведений и институтов повышения квалификации по подготовке и переподготовке кадров в области защиты информации.
21. Порядок рассекречивания конфиденциальных сведений, документов и изделий.
22. Методы проверки кандидатов на должности, связанные с работой с конфиденциальной информацией.
23. Организация контроля выполнения распорядка дня лицами, работающими на режимных объектах.
24. Каналы разглашения персоналом конфиденциальной информации.
25. Особенности осуществления охраны физических лиц.
26. Методика проектирования системы пропускного и внутриобъектового режимов и оценки эффективности их функционирования.
27. Порядок приема-сдачи под охрану режимных помещений.
28. Государственные, ведомственные и организационные нормативные акты, регламентирующие защиту государственной тайны в печати.
29. Использование аналитических методов при определении объектов и субъектов защиты и их взаимоотношений.
30. Особенности документирования процессов рассмотрения материалов и принятия решений.

#### **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 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;
- 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, 3,4,5,6);
- вопросы для рубежного контроля (модуль 1, 2, 3,4,5,6).

### **6.3 Итоговый контроль освоения заданных дисциплинарных компетенций**

#### **1) Зачёт**

Не предусмотрен.

#### **2) Экзамен**

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

Экзамен по дисциплине проводится устно по билетам. Билет содержит два теоретических вопроса по правовому или организационному обеспечению информационной безопасности, в зависимости от раздела изучения дисциплины.

Фонды оценочных средств, включающий типовые задания, задание на контрольную работу, тесты и методы оценки, критерии оценивания, перечень контрольных точек и таблица планирования результатов обучения, контрольные задания к экзаменам, позволяющие оценить результаты освоения данной дисциплины, входит в состав УМКД на правах отдельного документа.

Перечень экзаменационных вопросов:

1. Структура информационной сферы, характеристика ее элементов.
2. Информация как объект правоотношений, категории информации.
3. Система правовой защиты информации.
4. Понятие и виды защищаемой информации.
5. Особенности государственной тайны как защищаемой информации.
6. Система защиты государственной тайны.
7. Засекречивание информации, отнесенной к государственной тайне.
8. Защита сведений отнесенных к государственной тайне.
9. Понятие информации конфиденциального характера.
10. Основные виды конфиденциальной информации, в соответствии с требованиями российской нормативно-правовой базы.
11. Правовой режим конфиденциальной информации.
12. Основные требования, предъявляемые к организации защиты конфиденциальной информации.
13. Понятие и характеристика служебной тайны.

14. Нормативно - правовые основы защиты служебной тайны.
15. Порядок обращения с документами, содержащими служебную информацию ограниченного распространения.
16. Правовые основы защиты коммерческой тайны.
17. Виды информации, составляющей коммерческую тайну.
18. Права и обязанности обладателя коммерческой тайны.
19. Основные угрозы коммерческой тайны.
20. Правовая защита коммерческой тайны.
21. Правовые основы защиты банковской тайны.
22. Раскрытие информации, относящейся к банковской тайне.
23. Нарушение банковской тайны и ответственность за подобные нарушения.
24. Нотариальная тайна и ее особенности. Тайна завещания.
25. Врачебная тайна и ее особенности.
26. Адвокатская тайна и ее особенности.
27. Тайна страхования и ее особенности.
28. Тайна связи и ее особенности. Тайна переписки, почтовых, телеграфных и иных сообщений.
29. Тайна усыновления (удочерения). Тайна исповеди.
30. Формирование российского законодательства в области защиты персональных данных.
31. Основные понятия и содержание закона РФ «О персональных данных».
32. Подзаконные нормативно-правовые документы о порядке правовой защиты персональных данных.
33. Государственный надзор и контроль обработки персональных данных, ответственность за нарушения российского законодательства в данной области.
34. Правовые основы лицензирования в области защиты информации.
35. Правовые основы сертификации в области защиты информации.
36. Особенности правонарушений в информационной сфере.
37. Преступления в сфере компьютерной информации: виды, состав.
38. Основы расследования преступлений в сфере компьютерной информации.
39. Правовая защита информационных систем.
40. Правовая защита результатов интеллектуальной деятельности.
41. Соотношение организационных мер защиты информации с мерами правового и технического характера.
42. Основные термины, связанные с организацией защиты информации.
43. Организационные меры, направленные на защиту государственной тайны.
44. Режим секретности как основной порядок деятельности в сфере защиты государственной тайны.
45. Особенности системы организационной защиты государственной тайны.
46. Распределение между уровнями государственного управления полномочий, управленческих функций и задач по защите государственной тайны.
47. Организация деятельности режимно-секретных органов.
48. Установление и изменение степени секретности сведений, отнесенных к государственной тайне.
49. Понятие «рассекречивание сведений». Основания для рассекречивания сведений.
50. Порядок допуска и доступа к государственной тайне. Основные принципы допускной работы.
51. Номенклатура должностей работников, подлежащих оформлению на допуск и порядок ее составления и утверждения.
52. Документальное оформление для отправки на согласование.
53. Процедура оформления и переоформления допусков и ее документирование, подлежащее согласованию с органами государственной безопасности.
54. Организация доступа к сведениям, составляющим государственную тайну.



55. Понятие «охрана». Цели и задачи охраны.
56. Объекты охраны: территория, здания, помещения, персонал, информационные ресурсы, материальные и финансовые ценности. Особенности их охраны.
57. Виды, способы и особенности охраны различных объектов.
58. Понятие о рубежах охраны. Многорубежная система охраны.
59. Факторы выбора методов и средств охраны.
60. Организация охраны объектов защиты в процессе их транспортировки.
61. Понятие «режим», цели и задачи режимных мероприятий. Виды режима.
62. Организация пропускного режима. Основные положения инструкции об организации пропускного режима и работе бюро пропусков.
63. Виды пропускных документов.
64. Порядок организации работы бюро пропусков.
65. Контрольно-пропускные пункты, их оборудование и организация работы.
66. Понятие «внутриобъектовый режим» и его общие требования.
67. Противопожарный режим и его обеспечение.
68. Подбор и расстановка кадров.
69. Направления и методы работы с персоналом, обладающим конфиденциальной информацией. Организация обучения персонала.
70. Основные формы обучения и методы контроля знаний.
71. Мотивация персонала к выполнению требований по защите информации.
72. Основные формы воздействия на персонал как методы мотивации: вознаграждение, управление карьерой, профессиональная этика.
73. Организация контроля соблюдения персоналом требований режима защиты информации. Методы проверки персонала.
74. Организация служебного расследования по фактам разглашения персоналом конфиденциальной информации.
75. Организационные меры по защите информации при увольнении сотрудника.
76. Основные требования, предъявляемые к подготовке и проведению конфиденциальных переговоров.
77. Основные этапы проведения конфиденциальных переговоров.
78. Подготовка помещения для проведения конфиденциальных переговоров.
79. Подготовка программы проведения конфиденциальных переговоров.
80. Порядок проведения конфиденциальных переговоров.
81. Требования режима защиты информации при приеме в организации посетителей. Порядок доступа посетителей и командированных лиц к конфиденциальной информации. Порядок пребывания посетителей на территории и в помещениях организации.
82. Требования к программе приема иностранных представителей.
83. Требования к помещениям, в которых проводится прием иностранных представителей.
84. Обеспечение защиты информации при выезде за рубеж командированных лиц.
85. Основные виды и формы рекламы. Общие требования режима защиты информации в процессе рекламной деятельности.
86. Основные методы защиты информации в рекламной деятельности. Понятие «публикация в открытой печати». Общие требования режима защиты конфиденциальной информации при опубликовании материалов в открытой печати.
87. Особенности защиты информации при опубликовании материалов, определяемые характером деятельности организации, целями публикации, содержанием и характером публикации.
88. Концепция безопасности предприятия (организации) и ее содержание. Политика информационной безопасности.
89. Подразделения, обеспечивающие ИБ предприятия: основные функции, содержание деятельности, структура, обязанности сотрудников.
90. Основные документы службы информационной безопасности.

*Пример экзаменационного билета:*

<p><b>ПЕРМСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ</b>          Электротехнический факультет          Кафедра автоматики и телемеханики</p> <p>Экзамен по дисциплине «<b>Организационное и правовое обеспечение информационной безопасности</b>»</p> <p><b>Экзаменационный билет № 1</b></p> <p>1. Основные требования, предъявляемые к организации защиты конфиденциальной информации.</p> <p>2. Преступления в сфере компьютерной информации: виды, состав.</p> <p>Заведующий кафедрой д-р техн. наук, профессор</p> <p>А.А. Южаков</p>
--

#### 6.4 Виды 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 контроля					
	ТО	РТ	КР	ПЗ	От	Экз
1	2	3	4	5	6	7
<p><b>В результате освоения дисциплины студент</b>  <b>Знает:</b></p> <ul style="list-style-type: none"> <li>– основы российской правовой системы и законодательства, правового статуса личности, организации деятельности органов государственной власти Российской Федерации по защите информации;</li> <li>– характеристику основных отраслей российского права, правовые основы обеспечения национальной безопасности РФ;</li> <li>– виды и степень ответственности за правонарушения и преступления в информационной сфере;</li> <li>– порядок работы с персоналом по вопросам обеспечения защиты информации ограниченного доступа, проведения мероприятий по физической и технической защите конфиденциальной информации, организации службы безопасности предприятия;</li> <li>– основы организационного и правового обеспечения информационной безопасности, основные нормативные правовые акты в области обеспечения информационной безопасности и нормативные методические документы ФСБ России и ФСТЭК России в области защиты информации;</li> <li>– правовые основы организации защиты государственной тайны и конфиденциальной информации, задачи органов защиты государственной тайны и служб защиты информации на предприятиях;</li> </ul>	+	+				+
	+	+				+
	+	+				+
	+	+				+
	+	+				+

1	2	3	4	5	6	7
<p><b>Умеет:</b></p> <ul style="list-style-type: none"> <li>– определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите;</li> <li>– анализировать правовые акты и осуществлять правовую оценку информации;</li> <li>– предпринимать необходимые меры по восстановлению нарушенных прав;</li> <li>– организовывать работы по проверке кандидатов на должность, текущую работу с персоналом по обеспечению информационной безопасности;</li> <li>– разрабатывать проекты нормативных и организационно-распорядительных документов, регламентирующих работу по защите информации;</li> <li>– применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности;</li> </ul>			+	+		+
			+	+		+
			+	+		+
			+	+		+
			+	+		+
				+	+	+
				+	+	+
				+	+	+
<p><b>Владеет:</b></p> <ul style="list-style-type: none"> <li>– навыками поиска нормативной правовой информации, необходимой для профессиональной деятельности навыками работы с нормативными правовыми актами;</li> <li>– навыками работы с персоналом, принятия организационно-управленческих решений, в том числе в нестандартных ситуациях в целях обеспечения информационной безопасности;</li> <li>– навыками организации охраны объектов информатизации и обеспечения режима секретности, организации и управления деятельностью службы защиты информации на предприятии.</li> </ul>				+	+	+
				+	+	+
				+	+	+

ТО – текущий опрос (контроль знаний по теме);

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

КР – рубежная контрольная работа по модулю (оценка умений);

ПЗ – практические задания на групповых занятиях (оценка умений и владений);

От – публичная защита результатов отчёта на групповом занятии, в соответствии с индивидуальным заданием по модулю (оценка владения).



**8. Учебно-методическое и информационное обеспечение дисциплины**  
**8.1. Карта обеспеченности дисциплины учебно-методической литературой**

<b>Организационное и правовое обеспечение информационной безопасности</b> <i>полное название дисциплины</i>	<b>Профессиональный</b>													
	<input checked="" type="checkbox"/> основная <input type="checkbox"/> по выбору студента	<input checked="" type="checkbox"/> базовая часть цикла <input type="checkbox"/> вариативная часть цикла												
<b>090900.62</b> <b>090303.65</b> <i>код направления / специальности</i>	<b>«Информационная безопасность»</b> <b>«Информационная безопасность автоматизированных систем»</b> <i>полное название направления/ специальности</i>													
<b>КЗИ, КОБ</b>	Уровень подготовки <table border="1"> <tr><td><input checked="" type="checkbox"/></td><td>специалист</td></tr> <tr><td><input checked="" type="checkbox"/></td><td>бакалавр</td></tr> <tr><td><input type="checkbox"/></td><td>магистр</td></tr> </table>	<input checked="" type="checkbox"/>	специалист	<input checked="" type="checkbox"/>	бакалавр	<input type="checkbox"/>	магистр	Форма обучения <table border="1"> <tr><td><input checked="" type="checkbox"/></td><td>очная</td></tr> <tr><td><input type="checkbox"/></td><td>заочная</td></tr> <tr><td><input type="checkbox"/></td><td>очно-заочная</td></tr> </table>	<input checked="" type="checkbox"/>	очная	<input type="checkbox"/>	заочная	<input type="checkbox"/>	очно-заочная
<input checked="" type="checkbox"/>	специалист													
<input checked="" type="checkbox"/>	бакалавр													
<input type="checkbox"/>	магистр													
<input checked="" type="checkbox"/>	очная													
<input type="checkbox"/>	заочная													
<input type="checkbox"/>	очно-заочная													
<u>2013</u>	семестр (ы) <u>5,6</u>	количество групп <u>2</u> количество студентов <u>40</u>												

Шабуров Андрей Сергеевич, доцент,  
 электротехнический факультет,  
 кафедры АТ, телефон: 239-18-16.

Карта книго-  
 обеспеченности  
 в библиотеку сдана

## СПИСОК ИЗДАНИЙ

№	Библиографическое описание	Количество экземпляров в библиотеке
1	2	3
<b>1. Основная литература</b>		
1	Казанцев С.Я. Правовое обеспечение информационной безопасности. - М.: Академия, 2005. - 239 с.	18
2	Романов О. А., Бабин С. А., Жданов С. Г. Организационное обеспечение информационной безопасности: учебник для вузов. - М.: Академия, 2008. — 189 с.	7
3	Данилов А.Н., Шабуров А.С. Правовое обеспечение информационной безопасности. Учебное пособие.- Пермь: Изд-во ПГТУ, 2008. - 270 с.	100
4	Данилов А.Н., Шабуров А.С. Организационное обеспечение информационной безопасности. Учебное пособие. - Пермь: Изд-во ПГТУ, 2007. - 257 с.	100
<b>2. Дополнительная литература</b>		
<b>2.1. Учебные и научные издания</b>		
1	Городов О.А. Информационное право: учебник, М.: Проспект, 2009.— 242 с.	3
2	Бачило И.Л. Информационное право СПб: Изд-во Р. Асланова, 2005 — 723 с.	3
3	Тедеев А.А. Информационное право (право Интернета) М. : Эксмо, 2005 — 302 с.	6
4	Белов В.В. Интеллектуальная собственность. Законодательство и практика применения. - М.: Юристъ, 2006. - 351 с.	2
5	Праскурин Г.А. Организационное обеспечение информационной безопасности: курс лекций. - Томск: Изд-во ТУСУР, 2005. Ч. 1. - 2005. - 221 с.	5
6	Праскурин Г.А. Организационное обеспечение информационной безопасности: курс лекций. - Томск : Изд-во ТУСУР, Ч. 2, 2005. - 180 с.	5
7	Ярочкин В. И. Информационная безопасность: учебник для вузов, 5-е изд. - М: Акад. проект, 2008. - 543 с.	21
<b>2.2. Периодические издания</b>		
1	Интеллектуальная собственность (Авторское право)	
2	Интеллектуальная собственность (Промышленная собственность)	
<b>2.3. Нормативно-технические издания</b>		
<b>2.4. Официальные издания</b>		

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

Карта книго-  
обеспеченности  
в библиотеку срана

## Текущие данные об обеспеченности на \_\_\_\_\_

(дата контроля литературы)

Основная литература  обеспечена  не обеспеченаДополнительная литература  обеспечена  не обеспеченаЗав. 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-справочные и поисковые системы – Деловая пресса - www.businesspress.ru; – Гарант - www.garant.ru; – Информационно-справочная система «Консультант Плюс».	б/н	Получение правовой информации

**8.3 Программные инструментальные средства**

Не предусмотрены

**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

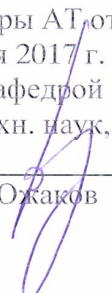
№ п.п.	Помещения			Площадь, м <sup>2</sup>	Количество посадочных мест
	Название	Принадлежность (кафедра)	Номер аудитории		
1	Дисплейный класс	Кафедра АТ	308 корп. А	34	18

**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	ПК Intel Pentium Dual CPU 2000 МГц	6	Оперативное управление	308 корп. А

**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, 7-11) внесены на основании перехода на ФГОС ВО:</b></p> <p><b>по направлению подготовки 10.03.01, утвержденный приказом Министерства образования и науки РФ от 01.12.2016 г. № 1515, и обновления базового учебного плана подготовки бакалавров по направлению 10.03.01, утвержденного 22.16.2016 г.:</b></p> <ul style="list-style-type: none"> <li>– общекультурную компетенцию ОК-1 считать общекультурной компетенцией ОК-5 с формулировкой: «Способность понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики»;</li> <li>– изменить шифр дисциплинарной компетенции с ОК-1.Б3.Б4 на ОК-5.Б1.Б.25;</li> <li>– общекультурную компетенцию ОК-5 считать общекультурной компетенцией ОК-6 с формулировкой: «Способность работать в коллективе, толерантно воспринимая социальные, культурные и иные различия»;</li> <li>– изменить шифр дисциплинарной компетенции с ОК-5.Б3.Б4 на ОК-6.Б1.Б.25;</li> <li>– профессиональную компетенцию ПК-4 считать общепрофессиональной компетенцией ОПК-5 с формулировкой «Способностью использовать нормативные правовые акты в профессиональной деятельности»;</li> <li>– изменить шифр дисциплинарной компетенции с ПК-4.Б3.Б4 на ОПК-5.Б1.Б.25;</li> </ul> <p><b>по специальности 10.05.03, утвержденный приказом Министерства образования и науки РФ от 01.12.2016 г. № 1509, и обновления базового учебного плана подготовки по специальности 10.05.03, утвержденного 22.16.2016 г.:</b></p> <ul style="list-style-type: none"> <li>– общекультурную компетенцию ОК-1 считать общекультурной компетенцией ОК-4 с формулировкой «Способность понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, со-</li> </ul>	<p>Протокол заседания кафедры АТ от «16 » января 2017 г. № 18 Зав. кафедрой АТ д-р техн. наук, проф.</p> <p>_____</p> <p>А.А. Южаков</p> 



блюдать нормы профессиональной этики»;

- изменить шифр дисциплинарной компетенции с ОК-1.С3.Б4 на ОК-4.Б1.Б22;
- изменить формулировку общекультурной компетенции ОК-6: «Способность работать в коллективе, толерантно воспринимая социальные, культурные и иные различия»;
- изменить шифр дисциплинарной компетенции с ОК-6. С3.Б4 на ОК-6.Б1.Б.22;
- профессиональную компетенцию ПК-6 считать общепрофессиональной компетенцией ОПК-6 с формулировкой «Способность применять нормативные правовые акты в профессиональной деятельности»;
- изменить шифр дисциплинарной компетенции с ПК-6.С3.Б4 на ОПК-6.Б1.Б22.

Наименование раздела 1.4 «Место учебной дисциплины в структуре профессиональной подготовки выпускников» изложить в следующей редакции: «Место учебной дисциплины в структуре образовательной программы».

В первом абзаце раздела 1.4 заменить слова «цикла профессиональных дисциплин» на «блока 1. Дисциплины (модули)». Шифр названия направления и специальности читать в новой редакции.

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».

Раздел 3 «Структура учебной дисциплины по видам и формам учебной работы» дополнить новым абзацем следующего содержания: «Объем дисциплины в зачетных единицах составляет 4 ЗЕ. Количество часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся указано в таблице 3.1.».

В табл. 3.1.:

- а) строку п. 1 дополнить словами «(контактная работа)»;
- б) строку п. 3 изложить в следующей редакции: «Итоговый контроль (промежуточная аттестация обучающихся) по дисциплине:».

В табл. 4.1.:

- а) в строке п. 1 «Количество часов (очная форма обучения)» дополнить словами «и виды занятий»;
- б) «Итоговая аттестация» заменить на «Итоговый контроль (промежуточная аттестация)».

В раздел 4.5 «Распределение тем по видам самостоятельной работы» добавить параграф с наименованием «Методические указания для обучающихся по изучению дисциплины» следующего содержания:

«При изучении дисциплины обучающимся целесообразно выполнять следующие рекомендации:

1. Изучение учебной дисциплины должно вестись систематически.

<p>2. После изучения какого-либо раздела по учебнику или конспектным материалам рекомендуется по памяти воспроизвести основные термины, определения, понятия раздела.</p> <p>3. Особое внимание следует уделить выполнению отчетов по практическим занятиям, лабораторным работам и индивидуальным комплексным заданиям на самостоятельную работу.</p> <p>4. Изучение дисциплины осуществляется в течение одного семестра, график изучения дисциплины приводится п. 7.</p> <p>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.»</p>	
<p>Наименование раздела 6 изложить в следующей редакции: «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: <b>Электронная библиотека</b> Научной библиотеки Пермского 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. <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. <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 разделом 8.3 и наименование изложить в следующей редакции: «Перечень информационных техноло-</p>	

	<p>гий, используемых при осуществлении образовательного процесса по дисциплине».</p> <p>Раздел 8.3 «Программные инструментальные средства» считать разделом 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.		
6.		
7.		
8.		