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
«__» _____ 2015 г.

УНИФИЦИРОВАННЫЙ УЧЕБНО-МЕТОДИЧЕСКИЙ КОМПЛЕКС ДИСЦИПЛИНЫ

«Разработка и эксплуатация защищенных автоматизированных систем»

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

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

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

Курс: 4 **Семестр**: 7

Трудоёмкость:

Кредитов по рабочему учебному плану:	4	ЗЕ
Часов по рабочему учебному плану:	152	Ч

Виды контроля:

Экзамен: - **7 сем.** Зачёт: - Курсовой проект: - Курсовая работа: -

Пермь 2015 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
«Разработка и эксплуатация защищенных автоматизированных систем»
РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Направление подготовки:	10.03.01 Информационная безопасность,
Направленность (профиль) образовательной программы:	Комплексная защита объектов информатизации
Специальность:	10.05.03 Информационная безопасность автоматизированных систем
Специализация:	Обеспечение информационной безопасности распределенных информационных систем
Квалификация выпускника:	бакалавр, специалист
Выпускающая кафедра:	Автоматика и телемеханика
Форма обучения:	очная

Курс: 4 **Семестр:** 7

Трудоемкость:

Кредитов по рабочему учебному плану (БУП): 4
Часов по рабочему учебному плану (БУП): 144

Виды контроля:

Экзамен: - 7 Зачет: **- нет** Курсовой проект: **- нет** Курсовая работа: **- нет**

Пермь 2017 г.

Рабочая программа дисциплины «Разработка и эксплуатация защищенных автоматизированных систем» разработана на основании:

- федерального государственного образовательного стандарта высшего профессионального образования, утвержденного приказом Министерства образования и науки Российской Федерации от «28» октября 2009 г., № 496, по направлению подготовки 090900 Информационная безопасность (квалификация (степень) «бакалавр»);
- федерального государственного образовательного стандарта высшего профессионального образования утвержденного приказом Министерства образования и науки Российской Федерации «17» января 2011г. № 60, по направлению подготовки (специальности) 090303 «Информационная безопасность автоматизированных систем» (квалификация (степень) «специалист»);
- компетентностной модели выпускника ООП по направлению подготовки 090900.62 - «Информационная безопасность», профилю подготовки «Комплексная защита объектов информатизации», утвержденной «24» июня 2013 г.;
- компетентностной модели выпускника ООП по специальности 090303.65 - «Информационная безопасность автоматизированных систем», специализации «Обеспечение информационной безопасности распределенных информационных систем», утвержденной «24» июня 2013 г.;
- базового учебного плана очной формы обучения по направлению подготовки 090900.62 - «Информационная безопасность», профилю подготовки «Комплексная защита объектов информатизации» «29» августа 2011 г.
- базового 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: «Техническая защита информации», «Комплексная система защиты информации на предприятии».

Разработчик канд. техн. наук, доцент _____ Шабуров А.С.

Рецензент канд. техн. наук _____ Полшков А.В.

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
«30» 03 2015 г., протокол № 31
Председатель методической комиссии
электротехнического факультета,
канд. техн. наук, профессор _____ Гольдштейн А.Л.

СОГЛАСОВАНО
Начальник управления образовательных программ,
канд. техн. наук, доцент _____ Репецкий Д.С.

Рабочая программа дисциплины «Разработка и эксплуатация защищенных автоматизированных систем» 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:

Безопасность баз данных и операционных систем, Теория информационной безопасности и методология защиты информации, Управление информационной безопасностью, базового учебного плана образовательной программы высшего образования - программы бакалавриата по направлению 10.03.01 Информационная безопасность, направленности (профиля) Комплексная защита объектов информатизации;

Безопасность сетей ЭВМ, Метрология, стандартизация и сертификация, Информационная безопасность в банковской системе, Внутренний аудит систем защиты информации на соответствие стандартам, Информационная безопасность в экономике 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 - формирование компетентности в области разработки и эксплуатации автоматизированных систем в защищенном исполнении, отдельных компонентов автоматизированных систем, с учетом требований нормативно-технической и методической документации по обеспечению безопасности информации.

В процессе изучения дисциплины студент осваивает следующие компетенции по направлениям подготовки ВПО:

Таблица 1.1 Заданные ФГОС ВПО 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	ПК-10	способность администрировать подсистемы информационной безопасности объекта
			ПСК-1	способность к установке, настройке и эксплуатации компонентов системы защиты информации на объектах информатизации с учетом требований нормативно-технической документации
2.	090303.65	Информационная безопасность автоматизированных систем	ПК-18	способность участвовать в разработке защищенных автоматизированных систем по профилю своей профессиональной деятельности
			ПК-19	способность участвовать в разработке компонентов автоматизированных систем в сфере профессиональной деятельности

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

Унифицированная профессиональная компетенция (УПК-1)

Способность участвовать в разработке и администрировании защищенных автоматизированных систем по профилю своей профессиональной деятельности

Унифицированная профессиональная компетенция (УПК-2)

Способность участвовать в разработке и эксплуатации компонентов автоматизированных систем на объектах информатизации в сфере профессиональной деятельности, с учетом требований нормативно-технической документации

Таблица 1.2 Обоснование разработки унифицированных компетенций

№	Направление подготовки		Соответствие унифицированной компетенции и базовой компетенции ФГОС ВПО	
	Код	Наименование	**Способность участвовать в разработке и администрировании защищенных автоматизированных систем по профилю своей профессиональной деятельности (УПК-1)**	**Способность участвовать в разработке и эксплуатации компонентов автоматизированных систем на объектах информатизации в сфере профессиональной деятельности, с учетом требований нормативно-технической документации (УПК-2)**
1.	090900.62	Информационная безопасность	способностью администрировать подсистемы информационной безопасности объекта (ПК-10)	Способность к установке, настройке и эксплуатации компонентов системы защиты информации на объектах информатизации с учетом требований нормативно-технической документации (ПСК-1)
2.	090303.65	Информационная безопасность автоматизированных систем	Способность участвовать в разработке защищенных автоматизированных систем по профилю своей профессиональной деятельности (ПК-18)	Способность участвовать в разработке компонентов автоматизированных систем в сфере профессиональной деятельности (ПК-19)

1.2. Задачи дисциплины:

- изучение основных угроз безопасности информации в автоматизированных системах и освоение методик оценки данных угроз;
- изучение методов, способов, средств, последовательности и содержания этапов разработки автоматизированных систем и подсистем безопасности автоматизированных систем;
- изучение основных мер по защите информации в автоматизированных системах;
- изучение содержания и порядка деятельности персонала по эксплуатации защищенных автоматизированных систем и подсистем безопасности автоматизированных систем.

После изучения дисциплины обучающийся должен демонстрировать следующие результаты:

знать:

- модели данных, систем и процессов защиты информации в автоматизированных системах;
- критерии оценки защищенности автоматизированных систем;

- основные угрозы безопасности информации и модели нарушителя в автоматизированных системах;
- методы, способы, средства, последовательность и содержание этапов разработки автоматизированных систем и подсистем безопасности автоматизированных систем;
- основные меры по защите информации в автоматизированных системах;
- содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и подсистем безопасности автоматизированных систем;
- методы и модели анализа угроз безопасности подсистем автоматизированных систем;
- состав работ по защите информации на стадиях и этапах создания автоматизированных систем, с учетом требований нормативно-технической документации;
- методы, способы и средства обеспечения отказоустойчивости автоматизированных систем;
- средства автоматизации проектирования автоматизированных систем;

уметь:

- разрабатывать модели нарушителей и оценивать угрозы информационной безопасности автоматизированных систем;
- выявлять уязвимости информационно-технологических ресурсов автоматизированных систем;
- определять комплекс мер для обеспечения информационной безопасности автоматизированных систем;
- выполнять работы по эксплуатации компонентов автоматизированных систем на объектах информатизации;

владеть:

- навыками анализа и синтеза структурных и функциональных схем защищенных автоматизированных информационных систем;
- методами и технологиями проектирования, моделирования, исследования подсистем безопасности автоматизированных систем.

1.3. Предметом освоения дисциплины являются следующие объекты:

- модели данных, систем и процессов защиты информации;
- стандарты оценки защищенности автоматизированных систем;
- критерии оценки защищенности автоматизированных систем;
- угрозы безопасности информации в автоматизированных системах;
- базовая модель угроз безопасности информации;
- модель нарушителя в автоматизированной системе;
- методы и модели оценки угроз безопасности автоматизированных систем;
- стадии и этапы разработки автоматизированных систем;
- средства автоматизации проектирования автоматизированных систем;
- состав работ по защите информации на стадиях и этапах создания автоматизированных систем;
- меры по защите информации в автоматизированных системах;
- содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и подсистем безопасности автоматизированных систем;
- методы, способы и средства обеспечения отказоустойчивости.

1.4. Место дисциплины в структуре профессиональной подготовки выпускников

Дисциплина «Разработка и эксплуатация защищенных автоматизированных систем» относится к вариативной части цикла профессиональных дисциплин по направлению 090900 Информационная безопасность (квалификация (степень) «бакалавр») и к базовой части цикла профессиональных дисциплин специальности 090303 Информационная безопасность автоматизированных систем (квалификация (степень) «специалист»).

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

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

Таблица 1.3. – Дисциплины, направленные на формирование компетенций

Код	Наименование компетенций	Предшествующие дисциплины	Последующие дисциплины
УПК-1	Способность участвовать в разработке и администрировании защищенных автоматизированных систем по профилю своей профессиональной деятельности	Технические средства охраны Программно-аппаратные средства защиты информации	Комплексная защита информации на предприятии
УПК-2	Способность участвовать в разработке и эксплуатации компонентов автоматизированных систем на объектах информатизации в сфере профессиональной деятельности, с учетом требований нормативно-технической документации	Техническая защита информации	Комплексная защита информации на предприятии Информационная безопасность в банковской системе

2. Требования к результатам освоения учебной дисциплины

Дисциплина обеспечивает формирование компетенций УПК-1 и УПК-2:

2.1. Дисциплинарная карта компетенции УПК-1

Код УПК-1	**Формулировка унифицированной дисциплинарной компетенции** Способность участвовать в разработке и администрировании защищенных автоматизированных систем по профилю своей профессиональной деятельности

Требования к компонентному составу компетенции

Перечень компонентов	Виды учебной работы	Средства оценки
В результате освоения компетенции, студент знает: – модели данных, систем и процессов защиты информации в автоматизированных системах; – критерии оценки защищенности автоматизированных систем; – основные угрозы безопасности информации и модели нарушителя в автоматизированных системах; – методы, способы, средства, последовательность и содержание этапов разработки автоматизированных систем; – основные меры по защите информации в автоматизированных системах; – содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем;	Лекции Семинарские занятия Самостоятельная работа студентов по изучению теоретического материала Экзамен	Вопросы текущего, рубежного и итогового контроля
умеет: – разрабатывать модели нарушителей и оценивать угрозы информационной безопасности автоматизированных систем; – определять комплекс мер для обеспечения информационной безопасности автоматизированных систем;	Практические занятия Самостоятельная работа студентов по решению практических задач	Отчет за выполнение практических заданий на ПЗ Отчёт по индивидуальным заданиям по модулю Темы ПЗ и ИЗМ
владеет: – навыками анализа и синтеза структурных и функциональных схем защищенных автоматизированных информационных систем.	Самостоятельная работа студентов по решению практических задач Самостоятельная работа по индивидуальному заданию	Отчет за выполнение практических заданий на ПЗ Отчёт по индивидуальным заданиям по модулю Темы ПЗ и ИЗМ

2.2. Дисциплинарная карта компетенции УПК-2

Код УПК-2	**Формулировка унифицированной дисциплинарной компетенции** Способность участвовать в разработке и эксплуатации компонентов автоматизированных систем на объектах информатизации в сфере профессиональной деятельности, с учетом требований нормативно-технической документации

Требования к компонентному составу компетенции

Перечень компонентов	Виды учебной работы	Средства оценки
В результате освоения компетенции, студент знает: – методы и модели анализа угроз безопасности подсистем автоматизированных систем; – методы, способы, средства, последовательность и содержание стадий и этапов разработки подсистем безопасности автоматизированных систем; – состав работ по защите информации на стадиях и этапах создания автоматизированных систем, с учетом требований нормативно-технической документации; – методы, способы и средства обеспечения отказоустойчивости автоматизированных систем; – средства автоматизации проектирования автоматизированных систем; – содержание и порядок деятельности персонала по эксплуатации подсистем безопасности автоматизированных систем;	Лекции Семинарские занятия Самостоятельная работа студентов по изучению теоретического материала Экзамен	Вопросы текущего, рубежного и итогового контроля
умеет: – выявлять уязвимости информационно-технологических ресурсов автоматизированных систем; – выполнять работы по эксплуатации компонентов автоматизированных систем на объектах информатизации;	Практические занятия Самостоятельная работа студентов по решению практических задач	Отчет за выполнение практических заданий на ПЗ Отчёт по индивидуальным заданиям по модулю Темы ПЗ и ИЗМ
владеет: – методами и технологиями проектирования, моделирования, исследования подсистем безопасности автоматизированных систем.	Самостоятельная работа студентов по решению практических задач Самостоятельная работа по индивидуальному заданию	Отчет за выполнение практических заданий на ПЗ Отчёт по индивидуальным заданиям по модулю Темы ПЗ и ИЗМ

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 (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 – Объём и виды учебной работы

№ п.п.	Виды учебной работы	Трудоёмкость, ч	Форма представления результатов
1	2	3	4
1	**Аудиторная работа**	**54**	
	- в том числе в интерактивной форме	14	
	- лекции (Л)	24	конспект лекций
	- в том числе в интерактивной форме	4	
	- практические занятия (ПЗ), семинарские занятия (СЗ)	28	отчёт о выполнении
	- в том числе в интерактивной форме	10	
	Контроль самостоятельной работы (КСР)	2	
2	**Самостоятельная работа студентов** (СРС)	**62**	
	- самостоятельное изучение теоретического материала (ИТМ)	32	отчет по вопросам для текущего и рубежного контроля
	- выполнение индивидуальных заданий по модулю (ИЗМ)	30	отчёт о выполнении
3	Итоговая аттестация по дисциплине	**36**	**Экзамен**
4	**Трудоёмкость дисциплины, всего:** **в часах (ч)** **в зачётных единицах (ЗЕ)**	 **152** **4**	

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.	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	4	2	2		4	2	2		8
		3	4	2	2		6	2	4		10
		4	6,5	2	4	0,5	6	4	2		12,5
	Всего по модулю:		**18,5**	8	10	0,5	**20**	10	10		**38,5**
2	2	5	4	2	2		4	2	2		8
		6	4	2	2		4	2	2		8
		7	4	2	2		4	2	2		8
		8	4	2	2		6	4	2		10
		9	4,5	2	2	0,5	6	4	2		10,5
	Всего по модулю:		**20,5**	10	10	0,5	**24**	14	10		**44,5**
3	3	10	4	2	2		4	2	2		8
		11	4	2	2		6	2	4		10
		12	7	2	4	1	8	4	4		15
	Всего по модулю:		**15**	6	8	1	**18**	8	10		**33**
Итоговая аттестация											**36**
Итого			**54**	**24**	**28**	**2**	**62**	**32**	**30**	**36**	**152/4**

4.2. Содержание разделов и тем учебной дисциплины

Модуль 1. Требования защищенности автоматизированных систем в условиях актуальных угроз безопасности информации

Раздел 1. Требования защищенности автоматизированных систем в условиях актуальных угроз безопасности информации

АРС: Л - 8 ч, ПЗ, СЗ - 10 ч., КСР – 0,5 ч., СРС: ИТМ - 10 ч., ИЗМ (ИЗМ-1) - 10 ч.

Тема 1. История развития, назначение и роль автоматизированных систем. Введение в дисциплину. Основные понятия и положения защиты информации в автоматизированных системах. Этапы развития информационных и автоматизированных систем. Классификация задач, решаемых с использованием автоматизированных систем. Модели данных, систем и процессов защиты информации в автоматизированных системах. Требования к моделям защиты информации в автоматизированных системах.

Тема 2. Критерии оценки защищенности автоматизированных систем. Международные стандарты оценки защищенности. Оценка защищенности на основе отечественных стандартов. История формирования общих критериев. Общий подход к формированию критериев оценки безопасности информационных технологий. Модель разработки объекта оценки. Последовательность формирования требований и спецификаций. Понятие профиля защиты и его особенности. Требования общих критериев и результаты оценки.

Тема 3. Определение и содержание понятия угрозы безопасности автоматизированных систем. Особенности современных автоматизированных систем как объектов информационного воздействия, критерии оценки их защищенности. Уязвимости информационно-технологических ресурсов автоматизированных систем. Основные угрозы безопасности ин-

формации автоматизированных систем и их классификация. Понятие модели нарушителя в автоматизированной системе. Мониторинг угроз безопасности автоматизированных систем.

Тема 4. Оценка угроз безопасности автоматизированных систем. Цели и задачи оценки угроз безопасности автоматизированных систем. Понятие базовой модели угроз безопасности информации. Порядок разработки модели угроз и нарушителей информационной безопасности автоматизированных систем. Методы и модели анализа угроз. Базовая модель угроз информационной системы персональных данных и порядок ее использования. Оценка угроз безопасности информационных систем персональных данных.

Модуль 2. Разработка защищенных автоматизированных систем
Раздел 3. Разработка защищенных автоматизированных систем.
АРС: Л - 10 ч, ПЗ, СЗ - 10 ч., КСР – 0,5 ч., СРС: ИТМ - 14 ч., ИЗМ (ИЗМ-1) - 10 ч.

Тема 5. Стадии и этапы разработки автоматизированных систем. Жизненный цикл автоматизированной системы. Методы, способы, средства, последовательность и содержание стадий и этапов разработки автоматизированных систем и подсистем безопасности автоматизированных систем. Задачи и этапы проектирования автоматизированных систем. Методологии проектирования. Организация работ, функции заказчиков и разработчиков.

Тема 6. Автоматизированное проектирование. Понятие автоматизированного проектирования. Системы автоматизированного проектирования. Средства автоматизации проектирования автоматизированных систем: общая характеристика, назначение и возможности, классификация. Структура программного обеспечения САПР. Автоматизированные системы проектирования средств и подсистем безопасности.

Тема 7. Разработка автоматизированных систем в защищенном исполнении. Общие требования по разработке автоматизированных систем в защищенном исполнении. Требования к автоматизированной системе в защищенном исполнении. Работы на стадиях и этапах создания автоматизированных систем в защищенном исполнении. Требования по защите сведений о создаваемой автоматизированной системе.

Тема 8. Реализация моделей безопасности автоматизированных систем. Модель реализации многоуровневой защиты автоматизированной системы. Реализация «ядра безопасности». Основные меры по защите информации в автоматизированных системах (организационные, правовые, программно-аппаратные, криптографические, технические). Механизмы и методы защиты в распределенных автоматизированных системах. Архитектура механизмов защиты распределенных автоматизированных систем. Анализ и синтез структурных и функциональных схем защищенных автоматизированных информационных систем.

Тема 9. Особенности разработки информационных систем персональных данных. Общие требования по защите персональных данных. Состав и содержание организационных и технических мер по защите информационных систем персональных данных. Порядок выбора мер по обеспечению безопасности персональных данных. Требования по защите персональных данных, в соответствии с уровнем защищенности. Особенности защиты среды виртуализации.

Модуль 3. Эксплуатация защищенных автоматизированных систем.
Раздел 3. Эксплуатация защищенных автоматизированных систем.
АРС: Л - 6 ч, ПЗ, СЗ - 8 ч., КСР – 1 ч., СРС: ИТМ - 8 ч., ИЗМ (ИЗМ-1) - 10 ч.

Тема 10. Общие понятия по эксплуатации автоматизированных систем. Задачи и функции администрирования автоматизированных систем. Автоматизация управления сетью. Организация администрирования автоматизированных систем. Административный персонал и работа с пользователями. Управление, тестирование и эксплуатация автоматизированных систем. Методы, способы и средства обеспечения отказоустойчивости автоматизированных систем.

Тема 11. Администрирование информационной безопасности автоматизированных систем. Содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и подсистем безопасности автоматизированных систем. Общие обязанности администратора информационной безопасности автоматизированных систем. Защита носителей информации резервное копирование и восстановление данных. Сопровождение автоматизированных систем. Управление рисками и инцидентами управления безопасностью.

Тема 12. Особенности эксплуатации автоматизированных систем в защищенном исполнении. Анализ информационной инфраструктуры автоматизированной системы и ее безопасности. Разработка и ведение эксплуатационной документации защищенных автоматизированных систем. Перечень основных эксплуатационных документов защищенных автоматизированных систем. Акт ввода в эксплуатацию на автоматизированную систему. Технический паспорт на автоматизированную систему. Методы мониторинга и аудита, выявления угроз информационной безопасности автоматизированных систем.

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 (семинара)
1	1	Модели данных, систем и процессов защиты информации в автоматизированных системах (ПЗ)
2	2	Критерии оценки защищенности автоматизированных систем
3	3	Определение и содержание понятия угрозы безопасности автоматизированных систем
4	4	Порядок разработки модели угроз и нарушителей информационной безопасности автоматизированных систем
5	4	Оценка угроз безопасности информационных систем персональных данных (ПЗ)
6	5	Стадии и этапы разработки автоматизированных систем
7	6	Автоматизированные системы проектирования средств и подсистем безопасности (ПЗ)
8	7	Работы на стадиях и этапах создания автоматизированных систем в защищенном исполнении
9	8	Анализ и синтез структурных и функциональных схем защищенных автоматизированных информационных систем
10	9	Порядок разработки информационных систем персональных данных (ПЗ)
11	10	Задачи и функции администрирования автоматизированных систем
12	11	Обязанности администратора информационной безопасности автоматизированных систем
13	12	Особенности эксплуатации автоматизированных систем в защищенном исполнении
14	12	Особенности ведения эксплуатационной документации (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	ИТМ: Этапы развития информационных и автоматизированных систем	2
2	ИТМ: Понятие профиля защиты и его особенности	2
3	ИТМ: Мониторинг угроз безопасности автоматизированных систем	2
4	ИТМ: Базовая модель угроз информационной системы персональных данных	4
4	ИЗМ: В соответствии с заданием для модуля 1, п.п. 4.5.1	10
5	ИТМ: Организация работ, функции заказчиков и разработчиков	2
6	ИТМ: Структура программного обеспечения САПР	2
7	ИТМ: Требования по защите сведений о создаваемой автоматизированной системе	2
8	ИТМ: Архитектура механизмов защиты распределенных автоматизированных систем	2
9	ИТМ: Особенности защиты среды виртуализации	2
9	ИЗМ: В соответствии с заданием для модуля 2, п.п. 4.5.1	10
10	ИТМ: Методы, способы и средства обеспечения отказоустойчивости автоматизированных систем	2
11	ИТМ: Управление рисками и инцидентами управления безопасностью	4
12	ИТМ: Методы мониторинга и аудита, выявления угроз информационной безопасности автоматизированных систем	4
12	ИЗМ: В соответствии с заданием для модуля 3, п.п. 4.5.1	10
	Итого: в **ч** / в **ЗЕ**	**62/1,7**

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

Индивидуальное задание представляет собой модель автоматизированной (информационной) системы в защищенном исполнении. Разработка модели основывается на устанавливаемых, в соответствии с вариантом, требованиях по безопасности информации. Требования устанавливаются относительно класса защиты автоматизированной системы от несанкционированного доступа, уровня защищенности персональных данных, особенностей автоматизированной системы, а также угроз безопасности информации, характерных для данной системы. Последовательность разработки модели осуществляется поэтапно, в соответствии с последовательностью изучаемых разделов учебной дисциплины. Разработка модели осуществляется в соответствии с требованиями стандарта по созданию систем в защищенном исполнении.

Раздел 1, модуль 1

Тема 1. Общие требования по безопасности информации в автоматизированной системе.
Тема 2. Последовательность формирования требований по безопасности информации.
Тема 3.Разработка частной модели угроз безопасности информации.
Тема 4.Оценка угроз безопасности информации в автоматизированной системе.

Раздел 2, модуль 2

Тема 5. Организация работ по созданию автоматизированной системы.
Тема 6. Автоматизация проектирования автоматизированной системы.
Тема 7. Техническое задание на создание автоматизированной системы в защищенном исполнении.
Тема 8. Требования к автоматизированной системе по защите от НСД.
Тема 9.Требования к уровню защищенности ИС ПДн.

Раздел 3, модуль 3

Тема 10. Средства обеспечения отказоустойчивости автоматизированной системы.
Тема 11. Порядок выполнения обязанностей администратора информационной безопасности автоматизированной системы.
Тема 12. Эксплуатационная документация защищенной автоматизированной системы.

.

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 в автоматизированных системах.

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 компетенции 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.**
В результате освоения дисциплины студент					
Знает:					
– модели данных, систем и процессов защиты информации в автоматизированных системах;	+	+	+		+
– критерии оценки защищенности автоматизированных систем;	+	+	+		+
– основные угрозы безопасности информации и модели нарушителя в автоматизированных системах;	+	+	+		+
– методы, способы, средства, последовательность и содержание этапов разработки автоматизированных систем;	+	+	+		+
– основные меры по защите информации в автоматизированных системах;	+	+	+		+
– содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем;	+	+	+		+
– методы и модели анализа угроз безопасности подсистем автоматизированных систем;	+	+	+		+
– методы, способы, средства, последовательность и содержание стадий и этапов разработки подсистем безопасности автоматизированных систем;	+	+	+		+
– состав работ по защите информации на стадиях и этапах создания автоматизированных систем, с учетом требований нормативно-технической документации;	+	+	+		+
– методы, способы и средства обеспечения отказоустойчивости автоматизированных систем;	+	+	+		+
– средства автоматизации проектирования автоматизированных систем;	+	+	+		+
– содержание и порядок деятельности персонала по эксплуатации подсистем безопасности автоматизированных систем;	+	+	+		+

Умеет: – разрабатывать модели нарушителей и оценивать угрозы информационной безопасности автоматизированных систем; – определять комплекс мер для обеспечения информационной безопасности автоматизированных систем; – выявлять уязвимости информационно-технологических ресурсов автоматизированных систем; – выполнять работы по эксплуатации компонентов автоматизированных систем на объектах информатизации;			+ + + +	+ + + +	
Владеет: – навыками анализа и синтеза структурных и функциональных схем защищенных автоматизированных информационных систем; – методами и технологиями проектирования, моделирования, исследования подсистем безопасности автоматизированных систем.			+ +	+ +	

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**	
Раздел:	**1**						**2**							**3**					
Лекции	2		2		2	2	2	2		2		2	2	2	2		2		**24**
Практические, семинарские занятия (ПЗ, СЗ)		2		2	2		2	2	2		2	2	2	2	2	2	2	2	**28**
Самост. изучение теоретического материала		2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2		**32**
Вып. инд. заданий (ИЗМ)		2	2	2	2	2		2	2	2	2	2		2	2	2	2	2	**30**
КСР						0,5							0,5					1	**2**
Модуль:	**1**						**2**												
Контр. тестирование						+							+					+	
Дисциплин. контроль																			**Экз.**

8. Учебно-методическое и информационное обеспечение дисциплины

8.1. Карта обеспеченности дисциплины учебно-методической литературой

Разработка и эксплуатация защищенных автоматизированных систем	*Профессиональный цикл*	
полное название дисциплины	[x] обязат [ ] по выбору студента	[x] базовая часть цикла [x] вариативная часть цикла

090900.62 090303.65	**«Информационная безопасность»,** профиль «Комплексная защита объектов информатизации» **«Информационная безопасность автоматизированных систем»,** специализация «Обеспечение информационной безопасности распределенных информационных систем»
код направления / специальности	*полное название направления/ специальности*

ИБ/КЗИ, КОБ	Уровень подготовки	Форма обучения
	[x] специалист [x] бакалавр [ ] магистр	[x] очная [ ] заочная [ ] очно-заочная

2015 семестр(ы) 7 количество групп 2
количество студентов 40

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

СПИСОК ИЗДАНИЙ

№	Библиографическое описание	Количество экземпляров в библиотеке
1	2	3
1. Основная литература		
1	Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей: учебное пособие / В.Ф. Шаньгин.— М.: ФОРУМ: ИНФРА-М, 2008.— 415 с.	10
2	Безукладников И.И. Проектирование и эксплуатация автоматизированных систем диспетчерского управления объектами критической инфраструктуры современного города: учебное пособие для вузов / И. И. Безукладников, Е. Л. Кон, А. А. Южаков; Пермский национальный исследовательский политехнический университет.— Пермь : Изд-во ПНИПУ, 2012 .— 174 с.	5
3	Галатенко В.А. Основы информационной безопасности: учебное пособие для вузов / В. А. Галатенко; Интернет-университет информационных технологий; Под ред. В. Б. Бетелина .— 4-е изд.— Москва: ИНТУИТ: БИНОМ. Лаб. знаний, 2012.— 205 с.	2
4	Клейменов С.А. Администрирование в информационных системах : учебное пособие для вузов / С.А. Клейменов, В.П. Мельников, А.М. Петраков ; Под ред. В.П. Мельникова.— М. : Академия, 2008. — 271 с.	5
2. Дополнительная литература		
	2.1. Учебные и научные издания	
1	Зегжда Д.П. Основы безопасности информационных систем : учебное пособие для вузов / Д. П. Зегжда, А. М. Ивашко .— Москва : Горячая линия-Телеком, 2000.— 451 с.	18
2	Малюк А. А. Введение в защиту информации в автоматизированных системах : учебное пособие для вузов / А. А. Малюк, С. В. Пазизин, Н. С. Погожин .— 2-е изд .— Москва : Горячая линия-Телеком, 2004.— 146 с.	10

Основные данные об обеспеченности на _____
(дата составления рабочей программы)

Основная литература [x] обеспечена [ ] не обеспечена

Дополнительная литература [x] 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

Карта книго-
обеспеченности
в библиотеку орган

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 – Гарант - www. garant.ru; – Информационно-справочная система «Консультант Плюс».	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, $м^2$	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 кафедры. Подпись заведующего кафедрой
1.	Содержание стр. 1, кроме абзацев 6-9, изложить в редакции, приведенной на стр. 1а.	Протокол заседания кафедры АТ от «16 » января 2017 г. № 18 Зав. кафедрой АТ д-р техн. наук, проф. _____ А.А. Южаков
	Содержание стр. 2 (абзацы 1-5) изложить в редакции, приведенной на стр. 2а.	
	Изменения шифров и формулировок компетенций (стр. 3- 5, 7-9,) внесены на основании перехода на ФГОС ВО: **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.:** - профессиональную компетенцию ПК-10 считать компетенцией ПК-3 с формулировкой: «Способность администрировать подсистемы информационной безопасности объекта защиты»; - изменить шифр дисциплинарной компетенции с ПК-10.Б3.В9 на ПК-3.Б1.В.08; - профессионально-специализированную компетенцию ПСК-1 считать компетенцией ПСК-2 с формулировкой «Способность организовывать технологический процесс защиты информации ограниченного доступа в соответствии с действующими нормативными правовыми актами и нормативными методическими документами ФСБ России, ФСТЭК России»; - изменить шифр дисциплинарной компетенции с ПСК-1.Б3.В9 на ПСК-2.Б1.В.08; **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.:** - профессиональную компетенцию ПК-18 считать общекультурной компетенцией ПК-6 с формулировкой «Способность проводить анализ, предлагать и обосновывать выбор решений по обеспечению эффективного применения автоматизированных систем в сфере профессиональной деятельности»; - изменить шифр дисциплинарной компетенции с ПК-18.С3.Б16 на ПК-6.Б1.Б34; - профессиональную компетенцию ПК-19 считать профессиональной компетенции ПК-9 с формулировкой «Способность участвовать в разработке защищенных автоматизированных систем в сфере профессиональной деятельности»; - изменить шифр дисциплинарной компетенции с ПК-19.С3.Б16 на ПК-9.Б1.Б34.	

	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. 2. После изучения какого-либо раздела по учебнику или конспектным материалам рекомендуется по памяти воспроизвести основные термины, определения, понятия раздела. 3. Особое внимание следует уделить выполнению отчетов по практическим занятиям, лабораторным работам и индивидуальным комплексным заданиям на самостоятельную работу. 4. Изучение дисциплины осуществляется в течение одного семестра, график изучения дисциплины приводится п. 7. 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.»	

	Наименование раздела 6 изложить в следующей редакции: «Фонд оценочных средств дисциплины».	
	Наименование параграфа 6.1 изложить в редакции «Текущий и рубежный контроль освоения заданных дисциплинарных частей компетенций».	
	В параграф 6.1 добавить первый абзац следующего содержания: «Текущий контроль осуществляется путем устного опроса во время аудиторных занятий».	
	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».	
	Изменить название раздела «Список изданий» на «8.2. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины».	
	Добавить в таблицу 8.1 строку «2.5 Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины».	
	Дополнить п. 2.5 таблицы строками: **Электронная библиотека** 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: http://elib.pstu.ru/. – Загл. с экрана. **Лань** [Электронный ресурс: электрон. -библ. система: полнотекстовая база данных электрон. документов по гуманит., естеств., и техн. наукам] / Изд-во «Лань». – Санкт-Петербург: Лань, 2010- . – Режим доступа: http://e.lanbook.com/. – Загл. с экрана. **Консультант Плюс** [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.».	
	Раздел 8.2 «Компьютерные обучающие и контролирующие программы» считать разделом 8.3 и наименование изложить в следующей редакции: «Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине».	
	Раздел 8.3 «Программные инструментальные средства» считать разделом 8.4 «Перечень программного обеспечения, в том числе компьютерные обучающие и контролирующие программы».	
	Раздел 8.4 «Аудио- и видео-пособия» считать разделом 8.5.	
	Наименование раздела 9 изложить в следующей редакции: «Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине».	

2.		
3.		
4.		
5.		
6.		
7.		
8.		