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
«13» ____09_____ 2015 г.

УНИФИЦИРОВАННЫЙ УЧЕБНО-МЕТОДИЧЕСКИЙ КОМПЛЕКС ДИСЦИПЛИНЫ
«Комплексная защита информации на предприятии»

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: 3 ЗЕ
Часов по рабочему учебному плану: 114 Ч

Виды контроля:
Экзамен: - Зачёт: **7 сем.** 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
«Комплексная система защиты информации на предприятии»
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): **3**
Часов по рабочему учебному плану (БУП): **108**

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

Пермь 2017 г.

Рабочая программа дисциплины «Комплексная защита информации на предприятии» 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: «Организационное и правовое обеспечение информационной безопасности», «Разработка и эксплуатация защищенных автоматизированных систем», «Управление информационной безопасностью».

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 «Комплексная система защиты информации на предприятии» 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 сетей ЭВМ, Безопасность баз данных и операционных систем, Теория информационной безопасности и методология защиты информации, Безопасность жизнедеятельности, Техническая защита информации, Защита и обработка конфиденциальных документов, Внутренний аудит систем защиты информации на соответствие стандартам, Информационная безопасность в экономике, Организация и управление службой защиты информации на предприятии, Аудит информационной безопасности учебного плана образовательной программы высшего образования - программы бакалавриата по направлению 10.03.01 Информационная безопасность, направленности (профиля) Комплексная защита объектов информатизации;

Техническая защита информации, Технические средства охраны, Методы проектирования защищенных распределенных информационных систем, Технология построения защищенных распределенных приложений 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 комплексной системы защиты информации предприятия, на основе оценки угроз безопасности информации, способов моделирования, технологии организации, кадрового, технологического и нормативно-методического обеспечения, методах оценки эффективности подобных систем.

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-4	способность формировать комплекс мер по информационной безопасности с учетом его правовой обоснованности, административно-управленческой и технической реализуемости и экономической целесообразности
			ПСК-2	способность к проведению анализа и оценки состояния защищенности объектов информатизации, на основе действующих международных и отечественных стандартов по защите информации
2.	090303.65	Информационная безопасность автоматизированных систем	ПК-13	способность разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы
			ПК-18	способность участвовать в разработке защищенных автоматизированных систем по профилю своей 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 проводить анализ и оценку состояния защищенности объектов информатизации на основе разработанной модели угроз и модели нарушителя информационной безопасности, в соответствии с действующими международными и отечественными стандартами по защите информации

Унифицированная профессиональная компетенция (УПК-2)

Способность участвовать в разработке защищенных автоматизированных систем, формировании комплекса мер по защите информации объектов информатизации на предприятии и с учетом их 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 проводить анализ и оценку состояния защищенности объектов информатизации на основе разработанной модели угроз и модели нарушителя информационной безопасности, в соответствии с действующими международными и отечественными стандартами по защите информации (УПК-1)**	**Способность участвовать в разработке защищенных автоматизированных систем, формировании комплекса мер по защите информации объектов информатизации на предприятии и с учетом их правовой обоснованности, административно-управленческой и технической реализуемости и экономической целесообразности (УПК-2)**
1.	090900.62	Информационная безопасность	способность к проведению анализа и оценки состояния защищенности объектов информатизации, на основе действующих международных и отечественных стандартов по защите информации (ПСК-2)	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 разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы (ПК-13)	способность участвовать в разработке защищенных автоматизированных систем по профилю своей профессиональной деятельности (ПК-18)

1.2. Задачи дисциплины:

- изучение сущности, целей и задач комплексной системы защиты информации;
- изучение принципов и этапов разработки комплексной системы защиты информации;
- освоение технологии установления состава защищаемой информации и объектов защиты информации на предприятии;
- овладение методами оценки угроз безопасности информации;
- изучение параметров и структуры комплексной системы защиты информации;
- установление состава мероприятий по обеспечению функционирования комплексной системы защиты информации;
- изучение показателей и методик эффективности системы защиты информации.

После изучения дисциплины обучающийся должен демонстрировать следующие результаты:

знать:

- понятие, сущность, цели и задачи комплексной системы защиты информации;
- принципы организации и этапы разработки комплексной системы защиты информации;
- факторы, влияющие на организацию комплексной системы защиты информации;
- технологию определения состава защищаемой информации и объектов защиты;
- методы моделирования, анализа и оценки угроз защищаемой информации;
- виды моделей, описывающих процессы защиты информации;
- содержание технологического и организационного построения системы защиты информации на предприятии;
- состав мероприятий и условия, обеспечивающие функционирование системы защиты информации на предприятии;
- порядок кадрового, материально-технического и нормативно-методического обеспечения защиты информации на предприятии;
- порядок организации планирования и контроля комплексной системы защиты информации на предприятии;
- методику анализа эффективности системы защиты информации;
- порядок организации аттестации объектов информатизации по требованиям безопасности информации;

уметь:

- классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности;
- классифицировать и оценивать угрозы информационной безопасности для объекта информатизации;
- формировать комплекс мер по защите информации на предприятии и оценивать их эффективность на основе заданных требований по безопасности информации;
- разрабатывать проекты нормативных и организационно-распорядительных документов, регламентирующих работу по защите информации на предприятии;

владеть:

- методиками проверки защищенности объектов информатизации на соответствие требованиям безопасности информации;
- технологией разработки организационно-функциональной структуры и комплекса нормативно-методического обеспечения комплексной защиты информации на предприятии.

1.3. Предметом освоения дисциплины являются следующие объекты:

- система защиты информации;
- анализ и оценки угроз защищаемой информации;
- модель процессов защиты информации;
- технологическое и организационное построение системы защиты информации;
- кадровое, материально-техническое и нормативно-методическое обеспечение защиты информации на предприятии;
- планирование и контроль комплексной системы защиты информации на предприятии;
- эффективность системы защиты информации;
- аттестации объектов информатизации по требованиям безопасности информации.

1.4. Место дисциплины в структуре профессиональной подготовки выпускников

Дисциплина «Комплексная защита информации на предприятии» относится к вариативной 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 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 проводить анализ и оценку состояния защищенности объектов информатизации на основе разработанной модели угроз и модели нарушителя информационной безопасности, в соответствии с действующими международными и отечественными стандартами по защите информации	Техническая защита информации	Управление информационной безопасностью
УПК-2	Способность участвовать в разработке защищенных автоматизированных систем, формировании комплекса мер по защите информации объектов информатизации на предприятии и с учетом их правовой обоснованности, административно-управленческой и технической реализуемости и экономической целесообразности	Организационное и правовое обеспечение информационной безопасности	Разработка и эксплуатация защищенных автоматизированных систем

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 проводить анализ и оценку состояния защищенности объектов информатизации на основе разработанной модели угроз и модели нарушителя информационной безопасности, в соответствии с действующими международными и отечественными стандартами по защите информации

Требования к компонентному составу компетенции

Перечень компонентов	Виды учебной работы	Средства оценки
В результате освоения компетенции, студент знает: – понятие, сущность, цели и задачи комплексной системы защиты информации; – принципы организации и этапы разработки комплексной системы защиты информации; – факторы, влияющие на организацию комплексной системы защиты информации; – технологию определения состава защищаемой информации и объектов защиты; – методы моделирования, анализа и оценки угроз защищаемой информации; – методику анализа эффективности системы защиты информации;	Лекции Семинарские занятия Самостоятельная работа студентов по изучению теоретического материала Зачетное занятие	Вопросы текущего, рубежного и итогового контроля
умеет: – классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности; – классифицировать и оценивать угрозы информационной безопасности для объекта 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: – методиками проверки защищенности объектов информатизации на соответствие требованиям безопасности информации.	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 защищенных автоматизированных систем, формировании комплекса мер по защите информации объектов информатизации на предприятии и с учетом их правовой обоснованности, административно-управленческой и технической реализуемости и экономической целесообразности

Требования к компонентному составу компетенции

Перечень компонентов	Виды учебной работы	Средства оценки
В результате освоения компетенции, студент знает: – виды моделей, описывающих процессы защиты информации; – содержание технологического и организационного построения системы защиты информации на предприятии; – состав мероприятий и условия, обеспечивающие функционирование системы защиты информации на предприятии; – порядок кадрового, материально-технического и нормативно-методического обеспечения защиты информации на предприятии; – порядок организации планирования и контроля комплексной системы защиты информации на предприятии; – порядок организации аттестации объектов информатизации по требованиям безопасности информации;	Лекции Семинарские занятия Самостоятельная работа студентов по изучению теоретического материала Зачетное занятие	Вопросы текущего, рубежного и итогового контроля
умеет: – формировать комплекс мер по защите информации на предприятии и оценивать их эффективность на основе заданных требований по безопасности информации; – разрабатывать проекты нормативных и организационно-распорядительных документов, регламентирующих работу по защите информации на предприятии;	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: – технологией разработки организационно-функциональной структуры и комплекса нормативно-методического обеспечения комплексной защиты информации на предприятии.	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)	**60**	
	- самостоятельное изучение теоретического материала (ИТМ)	30	отчет по вопросам для текущего и рубежного контроля
	- выполнение индивидуальных заданий по модулю (ИЗМ)	30	отчёт о выполнении
3	Итоговая аттестация по дисциплине	зачет	
4	**Трудоёмкость дисциплины, всего:** **в часах (ч)** **в зачётных единицах (ЗЕ)**	**114** **3**	

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		4	2	2		8
		4	4,5	2	2	0,5	8	4	4		12,5
	Всего по модулю:		**16,5**	8	8	0,5	**20**	10	10		**36,5**
2	2	5	4	2	2		6	4	2		10
		6	4	2	2		6	2	4		10
		7	6,5	2	4	0,5	8	4	4		14,5
	Всего по модулю:		**14,5**	6	8	0,5	**20**	10	10		**34,5**
3	3	8	4	2	2		4	2	2		8
		9	4	2	2		4	2	2		8
		10	4	2	2		4	2	2		8
		11	4	2	2		4	2	2		8
		12	7	2	4	1	4	2	2		11
	Всего по модулю:		**23**	10	12	1	**20**	10	10		**43**
Итоговая аттестация											
Итого			**54**	**24**	**28**	**2**	**60**	**30**	**30**		**114/3**

4.2. Содержание разделов и тем учебной дисциплины

Модуль 1. Концептуальные основы разработки комплексной системы защиты информации и определения объектов защиты

Раздел 1. Концептуальные основы разработки комплексной системы защиты информации и определения объектов защиты

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

Тема 1. Введение в дисциплину. Сущность комплексной системы защиты информации и принципы ее организации. Цель, задачи дисциплины, значение ее для подготовки специалиста. Знания и умения студентов, которые должны быть получены в результате ее изучения. Понятие, сущность и назначение комплексной системы защиты информации, ее задачи для обеспечения деятельности предприятия. Принципы организации комплексной системы защиты информации.

Тема 2. Методологические и концептуальные основы комплексной системы защиты информации. Методология защиты информации и ее основные задачи. Уровень обеспечения безопасности информации. Достаточность защиты информации. Варианты построения комплексной системы защиты. Основные факторы, влияющие на организацию комплексной системы защиты информации. Характер и степень влияния различных факторов на организацию системы защиты информации.

Тема 3. Определение и нормативное закрепление информации ограниченного доступа. Классификация информации по видам тайны и степеням конфиденциальности. Этапы работы по выявлению состава защищаемой информации. Нормативное закрепление состава

защищаемой информации. Порядок организации нормативного закрепления информации ограниченного доступа.

Тема 4. Определение состава объектов защиты. Понятие объекта защиты. Последовательность определения объекта защиты. Значение носителей защищаемой информации как объектов защиты. Факторы, определяющие состав носителей информации. Сущность защищаемого объекта информатизации. Методика выявления состава носителей защищаемой информации. Основные и вспомогательные технические средства и системы. Особенности помещений как объектов защиты.

Модуль 2. Моделирование угроз безопасности информации и процессов защиты информации на предприятии.

Раздел 2. Моделирование угроз безопасности информации и процессов защиты информации на предприятии.

АРС: Л - 6 ч, ПЗ, СЗ - 8 ч., КСР – 0,5 ч., СРС: ИТМ - 10 ч., ИЗМ (ИЗМ-1) - 10 ч.

Тема 5. Источники, способы и результаты дестабилизирующего воздействия на информацию. Определение источников дестабилизирующего воздействия на информацию. Модель формирования множества дестабилизирующих факторов. Понятие угрозы безопасности информации. Базовая модель угроз безопасности информации. Классификация угроз безопасности информации для объекта информатизации. Анализ и оценка угроз информационной безопасности объекта.

Тема 6. Выявление каналов утечки и методов несанкционированного воздействия на информацию. Сущность утечки информации и несанкционированного воздействия на информацию. Структурная модель канала утечки информации. Технические каналы утечки информации и их классификация. Модель технических каналов утечки информатизации на типовом объекте информатизации. Каналы утечки из-за несанкционированного воздействия на информацию на системы, использующие информационно - коммуникационные технологии. Инсайдерские каналы утечки информации и «социальный инжиниринг» Методы «социального инжиниринга».

Тема 7. Моделирование процессов защиты информации. Понятие модели и объекта моделирования. Основные виды моделей и их характеристика. Задачи и этапы моделирования в процессе построения комплексной системы защиты информации. Понятие архитектуры системы защиты информации. Кибернетическая, функциональная, информационная и организационная модели комплексной системы защиты информации. Формальные модели безопасности. Теории и методы моделирования процессов защиты информации.

Модуль 2. Особенности построения комплексной системы защиты информации предприятия и оценка ее эффективности.

Раздел 3. Особенности построения комплексной системы защиты информации предприятия и оценка ее эффективности

АРС: Л - 10 ч, ПЗ, СЗ - 12 ч., КСР – 1 ч., СРС: ИТМ - 10 ч., ИЗМ (ИЗМ-1) - 10 ч.

Тема 8. Технологическое и организационное построение комплексной системы защиты информации. Общее содержание работ по организации комплексной системы защиты информации. Характеристика технологического и организационного направлений создания комплексной системы защиты информации. Содержание стадий построения комплексной системы защиты информации. Предпроектное обследование. Назначение и структура технического задания, технико-экономического обоснования. Технический проект, рабочий проект. Апробация системы защиты информации и ввод ее в эксплуатацию.

Тема 9. Кадровое, материально-техническое и нормативно-методическое обеспечение защиты информации. Кадровое обеспечение функционирования комплексной системы защиты информации. Защита человеческих ресурсов. Распределение функций по защите информации. Материально-техническое обеспечение защиты информации. Нормативно-методическое обеспечение комплексной защиты информации на предприятии. Порядок разработки нормативных и организационно-распорядительных документов, регламентирующих работу по защите информации на предприятии.

Тема 10. Планирование и контроль комплексной системы защиты информации. Понятие, принципы и методы планирования комплексной системы защиты информации. Стадии планирования. Факторы, влияющие на выбор принципов и способов планирования. Структура и общее содержание планов предприятия и функционирования комплексной системы защиты информации. Организация выполнения планов. Сущность, цель, задачи и содержание контроля комплексной системы защиты информации. Виды и методы контроля системы защиты информации. Основные контрольные мероприятия по защите информации.

Тема 11. Оценка эффективности комплексной системы защиты информации. Понятие эффективности и эффективности защиты информации. Требование по защите информации. Показатель и норма эффективности защиты информации. Подходы к оценке эффективности систем защиты информации и их особенности. Состав методов и моделей оценки эффективности систем защиты информации. Области применения различных методов и моделей для решения задач оценки эффективности системы защиты информации на предприятии. Методики проверки защищенности объектов информатизации на соответствие требованиям нормативных документов.

Тема 12. Аттестация объектов информатизации по требованиям безопасности информации. Состав и содержание нормативно - правовых актов по аттестации объектов информатизации. Система аттестации объектов информатизации по требованиям безопасности информации. Организация аттестационных испытаний. Типовое содержание аттестационных испытаний объектов информатизации. Аттестационные испытания автоматизированных систем на соответствие требованиям по защите информации от несанкционированного доступа Аттестационные испытания объектов вычислительной техники по требованиям безопасности информации от утечки по каналам побочных электромагнитных излучений и наводок. Аттестационные испытания выделенных помещений. Инструментальные средства для проведения аттестационных испытаний. Основы проведения поисковых мероприятий по выявлению закладочных устройств.

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	2	3
1	1	Комплексная система защиты информации на предприятии и принципы ее организации (СЗ)
2	2	Оценка факторов, влияющих на организацию комплексной системы защиты информации (ПЗ)
3	3	Этапы работы по выявлению состава защищаемой информации на предприятии (ПЗ)
4	4	Определение состава объектов защиты на предприятии (ПЗ)
5	5	Анализ и оценка угроз информационной безопасности объекта информатизации (ПЗ)

1	2	3
6	6	Выявление каналов утечки информации на предприятии (ПЗ)
7	7	Задачи и этапы моделирования в процессе построения комплексной системы защиты информации (СЗ)
8	7	Моделирование процессов защиты информации (ПЗ)
9	8	Технологическое и организационное построение комплексной системы защиты информации (СЗ)
10	9	Разработка нормативных и организационно-распорядительных документов, регламентирующих работу по защите информации на предприятии (ПЗ)
11	10	Организация планирования и контроля комплексной системы защиты информации на предприятии (СЗ)
12	11	Применение методов и моделей оценки эффективности систем защиты информации (ПЗ)
13	12	Состав и содержание нормативно - правовых актов по аттестации объектов информатизации (СЗ)
14	12	Организация и проведение процедур аттестации объектов информатизации по требованиям безопасности информации (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: Знания и умения студентов, которые должны быть получены в результате изучения дисциплины	2
2	ИТМ: Характер и степень влияния различных факторов на организацию системы защиты информации	2
3	ИТМ: Порядок организации нормативного закрепления информации ограниченного доступа	2
4	ИТМ: Особенности помещений как объектов защиты	4
4	ИЗМ: В соответствии с заданием для модуля 1, п.п. 4.5.1	10
5	ИТМ: Базовые модели угроз безопасности различных видов информации ограниченного доступа	4
6	ИТМ: Методы «социального инжиниринга»	2
7	ИТМ: Формальные модели безопасности	4
7	ИЗМ: В соответствии с заданием для модуля 2, п.п. 4.5.1	10
8	ИТМ: Апробация системы защиты информации и ввод ее в эксплуатацию	2
9	ИТМ: Порядок разработки нормативных и организационно-распорядительных документов, регламентирующих работу по защите информации на предприятии	2
10	ИТМ: Основные контрольные мероприятия по защите информации	2

1	2	3
11	ИТМ: Области применения различных методов и моделей для решения задач оценки эффективности системы защиты информации на предприятии	2
12	ИТМ: Основы проведения поисковых мероприятий по выявлению закладочных устройств	2
12	ИЗМ: В соответствии с заданием для модуля 3, п.п. 4.5.1	10
	Итого: в **ч** / в **ЗЕ**	**60/1,67**

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

Индивидуальное задание представляет собой набор структурно-функциональных моделей подсистем комплексной системы защиты информации на предприятии. Модели разрабатывается студентом самостоятельно, в течение всего учебного семестра и отражает необходимые требования по составу организационного и технологического состава мероприятий по защите информации на предприятии. Последовательность разработки моделей осуществляется поэтапно, в соответствии с последовательностью изучаемых разделов учебной дисциплины. Разработка моделей осуществляется в соответствии с требованиями стандарта по созданию систем защиты информации и оценки их эффективности.

Раздел 1, модуль 1

Тема 1. Определение основных бизнес-процессов на предприятии.

Тема 2. Определение факторов, влияющих на организацию комплексной системы защиты информации на предприятии.

Тема 3. Формирование перечня сведений конфиденциального характера на предприятии.

Тема 4. Определение объектов защиты на предприятии.

Раздел 2, модуль 2

Тема 5. Классификация угроз безопасности информации для объекта информатизации на предприятии.

Тема 6. Разработка модели технических каналов утечки информатизации на типовом объекте информатизации предприятия.

Тема 7. Разработка моделей подсистем защиты информации.

Раздел 3, модуль 3

Тема 8. Разработка технико-экономического обоснования комплексной системы защиты информации.

Тема 9. Разработка комплекта организационно-распорядительных документов, регламентирующих работу по защите информации на предприятии.

Тема 10. Разработка плана проведения контрольных мероприятий по защите информации на предприятии.

Тема 11. Разработка перечня мероприятий по оценке эффективности комплексной системы защиты информации на предприятии .

Тема 12. Разработка модели подготовки и организации аттестационных испытаний объекта информатизации предприятия.

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 (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**

Не предусмотрен.

2) **Зачет**

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

Зачет 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 зачету, 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	Зач.
В результате освоения дисциплины студент					
Знает:					
– понятие, сущность, цели и задачи комплексной системы защиты информации;	+	+	+		+
– принципы организации и этапы разработки комплексной системы защиты информации;	+	+	+		+
– факторы, влияющие на организацию комплексной системы защиты информации;	+	+	+		+
– технологию определения состава защищаемой информации и объектов защиты;	+	+	+		+
– методы моделирования, анализа и оценки угроз защищаемой информации;	+	+	+		+
– виды моделей, описывающих процессы защиты информации;	+	+	+		+
– содержание технологического и организационного построения системы защиты информации на предприятии;	+	+	+		+
– состав мероприятий и условия, обеспечивающие функционирование системы защиты информации на предприятии;	+	+	+		+
– порядок кадрового, материально-технического и нормативно-методического обеспечения защиты информации на предприятии;	+	+	+		+
– порядок организации планирования и контроля комплексной системы защиты информации на предприятии;	+	+	+		+
– методику анализа эффективности системы защиты информации;	+	+	+		+
– порядок организации аттестации объектов информатизации по требованиям безопасности информации;	+	+	+		+
Умеет:					
– классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности;			+	+	
– классифицировать и оценивать угрозы информационной безопасности для объекта информатизации;			+	+	
– формировать комплекс мер по защите информации на предприятии и оценивать их эффективность на основе заданных требований по безопасности информации;			+	+	
– разрабатывать проекты нормативных и организационно-распорядительных документов, регламентирующих работу по защите информации на предприятии;			+	+	
Владеет:					
– методиками проверки защищенности объектов информатизации на соответствие требованиям безопасности информации;			+	+	
– технологией разработки организационно-функциональной структуры и комплекса нормативно-методического обеспечения комплексной защиты информации на предприятии.			+	+	

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);
Зач. – (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		**30**
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**							**3**						
Контр. тестирование					+							+						+	
Дисциплин. контроль																			**Зач.**

8. Учебно-методическое и информационное обеспечение дисциплины

8.1. Карта обеспеченности дисциплины учебно-методической литературой

Комплексная защита информации на предприятии	*Профессиональный цикл*
полное название дисциплины	[x] обязат; [ ] по выбору студента; [ ] 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: [x] специалист; [x] бакалавр; [ ] магистр	Форма обучения: [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	Грибунин В.Г. Комплексная система защиты информации на предприятии : учебное пособие для вузов / В.Г. Грибунин В.В. Чудовский .— Москва : Академия, 2009 .— 412 с.	23
2	Гришина Н.В. Организация комплексной системы защиты информации / Н. В. Гришина.— М. : Гелиос АРВ, 2007 .— 255 с.	10
3	Обеспечение информационной безопасности машиностроительных предприятий : учебное пособие для вузов : в 2 ч. / С. А. Клейменов [и др.].— Старый Оскол : ТНТ, Ч. 1.— 2011.— 359 с.	1
	2. Дополнительная литература	
	2.1. Учебные и научные издания	
1	Садердинов А. А. Информационная безопасность предприятия : учебное пособие / А. А. Садердинов, В. А. Трайнев, А. А. Федулов ; Международная академия наук информации, информационных процессов и технологий.— Москва : Дашков и К, 2004 .— 336 с.	14
2	Северин В.А. Правовая защита информации в коммерческих организациях: учебное пособие для вузов / В.А. Северин; Под ред. Б.И. Пугинского.— Москва: Академия, 2009 .— 220 с.	4
3	Игнатьев В.А. Защита информации в корпоративных информационно-вычислительных сетях: монография / В. А. Игнатьев.— Старый Оскол: ТНТ, 2005.— 550 с.	1

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 сдана

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 – «Гарант» - www. garant.ru; – Информационно-справочная система «Консультант Плюс».	б/н	Получение правовой информации

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 1-7) изложить в редакции, приведенной на стр. 2а.	
	Изменения шифров и формулировок компетенций (стр. 3 - 5, 6-8,) 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-4 считать компетенцией ОПК-7 с формулировкой: «Способность определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты»; - изменить шифр дисциплинарной компетенции с ПК-4.Б3.В2 на ОПК-7.Б1.В.04; - профессионально-специализированную компетенцию ПСК-2 считать профессиональной компетенцией ПК-5 с формулировкой «Способность принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации»; - изменить шифр дисциплинарной компетенции с ПСК-2.Б3.В2 на ПК-5.Б1.В.04; **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-13 профессионально-специализированной компетенцией ПСК-7.1 с формулировкой «Способность разрабатывать и исследовать модели информационно-технологических ресурсов, разрабатывать модели угроз и модели нарушителя информационной безопасности в распределенных информационных системах»; - изменить шифр дисциплинарной компетенции с ПК-13.С3.В2 на ПСК-7.1.Б1.В02; - профессиональную компетенцию ПК-18 считать профессиональной компетенции ПК-8 с формулировкой «Способность разрабатывать и анализировать проектные решения по обеспечению безопасности автоматизированных систем»;	

	- изменить шифр дисциплинарной компетенции с ПК-18.С3.В2 на ПК-8.Б1.В02.	
	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 3 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 ли-	

	тературе) 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».	