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.

УЧЕБНО-МЕТОДИЧЕСКИЙ КОМПЛЕКС ДИСЦИПЛИНЫ
«Безопасность операционных систем»

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

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

Специализация специалиста	- 09030307.65 Обеспечение информационной безопасности распределенных информационных систем
Квалификация (степень) выпускника	- специалист
Специальное звание выпускника	- специалист по защите информации
Выпускающая кафедра	«Автоматика и телемеханика»
Форма обучения	очная

Курс: 4,5 Семестр: 8,9

Трудоёмкость:
Кредитов по рабочему учебному плану: 10 ЗЕТ
Часов по рабочему учебному плану: 288 АЧ

Виды контроля:
Экзамен: -9 Зачет: -8 Курсовой проект: - Курсовая работа: -8

Пермь 2015 г.

Рабочая программа дисциплины «Безопасность операционных систем» разработана на основании:

- Федерального государственного образовательного стандарта высшего профессионального образования утвержденного приказом Министерства образования и науки Российской Федерации «17» января 2011 г. № 60, по направлению подготовки (специальности) 090303 «Информационная безопасность автоматизированных систем» (квалификация (степень) «специалист»);
- Компетентностной модели (КМ) выпускника ООП по специализации подготовки 090303.07.65 - Обеспечение информационной безопасности распределенных информационных систем, утвержденной«24» июня 2013 г.;
- Рабочего учебного плана очной формы обучения по специализации подготовки 090303.07.65 - Обеспечение информационной безопасности распределенных информационных систем, (набор 2011 года), утвержденного «29» августа 2011 г.

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

Разработчик канд. техн. наук _____ Кокоулин А.Н.

Рецензент канд. техн. наук _____ Шабуров А.С.

Рабочая программа рассмотрена и одобрена на заседании кафедры «Автоматика и телемеханика» «17» января 2015 г., протокол № 17.
Заведующий кафедрой,
«Автоматика и телемеханика»,
д-р. техн. наук, профессор _____ Южаков А.А.

Рабочая программа одобрена методической комиссией электротехнического факультета
«25» июня 2015 г., протокол № 38
Председатель методической комиссии
электротехнического факультета,
канд. техн. наук, профессор _____ Гольдштейн А.Л.

СОГЛАСОВАНО
Заведующий выпускающей кафедрой
«Автоматика и телемеханика»
д-р техн. наук, профессор _____ А.А. Южаков

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

1. Общие положения

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

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

- Способность разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы (ПК-13);
- Способность проводить анализ рисков информационной безопасности автоматизированных систем (ПК-14);
- Способность разрабатывать политики информационной безопасности автоматизированных систем (ПК-20).

1.2. Задачи дисциплины:

– изучение основных положений, понятий и категорий международных правовых документов Конституции и нормативно-правовых актов Российской Федерации в области обеспечения информационной безопасности;

– изучение правовых основ и принципов организации защиты государственной тайны и конфиденциальной информации, задач органов защиты государственной тайны и служб защиты информации на предприятиях;

– ознакомление с политикой безопасности компании в области информационной безопасности;

– ознакомление со стандартами информационной безопасности;

– изучение криптографических методов и алгоритмов шифрования информации;

– изучение алгоритмов аутентификации пользователей;

– приобретение навыков защиты информации в сетях;

– изучение требований к системам защиты информации.

– приобретение умений в разработке проектов нормативных и организационно-распорядительных документов в области обеспечения информационной безопасности и их применении;

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

После изучения дисциплины обучающийся должен демонстрировать следующие результаты:

знать:

– 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, средства автоматизации проектирования автоматизированных систем;

– содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и подсистем безопасности автоматизированных систем;

– методы и модели анализа угроз безопасности подсистем автоматизированных систем; методы, способы и средства обеспечения отказоустойчивости автоматизированных систем;
– основные меры по защите информации в автоматизированных системах, состав работ по защите информации на стадиях и этапах создания автоматизированных систем, с учетом требований нормативно-технической документации;

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 «Безопасность операционных систем» относится к базовой части цикла профессиональных дисциплин по специальности 090303 Информационная безопасность автоматизированных систем (квалификация (степень) «специалист»).

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

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

Таблица 1.1 - Дисциплины, направленные на формирование компетенций

Направление (специальность)	**Код компетенции**	**Наименование компетенций**	**Предшествующие дисциплины**	**Последующие дисциплины**
090303.65	ПК-13	Способность разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированных систем	Основы построения инфокоммуникационных систем и сетей Вычислительная техника и информационные технологии	Информационная безопасность в экономике
	ПК-14	Способность проводить анализ рисков информационной безопасности автоматизированных систем	Основы построения инфокоммуникационных систем и сетей Защита и обработка конфиденциальных документов	Управление информационной безопасностью
	ПК-20	Способность разрабатывать политики информационной безопасности автоматизированных систем	Основы построения инфокоммуникационных систем и сетей Вычислительная техника и информационные технологии	Защита и обработка конфиденциальных документов Информационная безопасность в банковской системе

2. Требования к результатам освоения учебной дисциплины

Дисциплина обеспечивает формирование части компетенции ПК-13,ПК-14 и ПК-20:

2.1. Дисциплинарная карта компетенции ПК-13

Код ПК-13	**Формулировка компетенции** Способность разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированных систем

Код ПК-13 .С3.Б19	**Формулировка дисциплинарной части компетенции:** Способность организовывать проведение и сопровождать аттестацию информационных систем в соответствии с требованиями государственных или корпоративных нормативных документов

Требования к компонентному составу части компетенции

Требования к компонентному составу компетенции

Перечень компонентов	Виды учебной работы	Средства оценки
В результате освоения компетенции, студент знает: – содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и подсистем безопасности автоматизированных систем; (ПК-13 .С3.Б19.1З) – основные меры по защите информации в автоматизированных системах, состав работ по защите информации на стадиях и этапах создания автоматизированных систем, с учетом требований нормативно-технической документации; (ПК-13 .С3.Б19.2З)	Лекции Семинарские занятия Самостоятельная работа студентов по изучению теоретического материала	Вопросы текущего, рубежного и итогового контроля; собеседование по самостоятельно изученному материалу
умеет: – определять комплекс мер для обеспечения информационной безопасности автоматизированных систем; (ПК-13 .С3.Б19.1У) – выполнять работы по эксплуатации компонентов автоматизированных систем на объектах информатизации; (ПК-13 .С3.Б19.2У)	Практические занятия; выполнение индивидуального задания по тематике практических занятий	Темы индивидуального задания по тематике практических занятий
владеет: – методами и технологиями проектирования, моделирования, исследования подсистем безопасности автоматизированных систем. (ПК-13 .С3.Б19.1В)	Самостоятельная работа по индивидуальному заданию по учебному модулю дисциплины	Те мы индивидуальных заданий по учебному модулю дисциплины

2.2. Дисциплинарная карта компетенции ПК-14

Код ПК-14	**Формулировка унифицированной дисциплинарной компетенции** Способность проводить анализ рисков информационной безопасности автоматизированных систем

Код ПК-14 .С3.Б19	**Формулировка дисциплинарной части компетенции:** Способность принимать участие в проведении экспериментально-исследовательских работ по установке, настройке и аудиту системы защиты информации с учетом особенностей операционных систем, баз данных и сетей передачи данных

Требования к компонентному составу части компетенции

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; (ПК-14 .С3.Б19.1З) – основные угрозы безопасности информации и модели нарушителя в автоматизированных системах; (ПК-14 .С3.Б19.2З)	Лекции Семинарские занятия Самостоятельная работа студентов по изучению теоретического материала	Вопросы текущего, рубежного и итогового контроля; собеседование по самостоятельно изученному материалу
умеет: – определять комплекс мер для обеспечения информационной безопасности автоматизированных систем; (ПК-14 .С3.Б19.1У)	Практические занятия; выполнение индивидуального задания по тематике практических занятий	Темы индивидуального задания по тематике практических занятий
владеет: – методами и технологиями проектирования, моделирования, исследования подсистем безопасности автоматизированных систем. (ПК-14 .С3.Б19.1В)	Самостоятельная работа по индивидуальному заданию по учебному модулю дисциплины	Те мы индивидуальных заданий по учебному модулю дисциплины

2.3. Дисциплинарная карта компетенции ПК-20

Код ПК-20	**Формулировка унифицированной дисциплинарной компетенции** Способность разрабатывать политики информационной безопасности автоматизированных систем

Код ПК-20 .С3.Б19	**Формулировка дисциплинарной части компетенции:** Способность разрабатывать политики информационной безопасности автоматизированных систем с учетом особенностей операционных систем, баз данных и сетей передачи данных

Требования к компонентному составу части компетенции

Требования к компонентному составу компетенции

Перечень компонентов	Виды учебной работы	Средства оценки
В результате освоения компетенции, студент знает: – методы, способы, средства, последовательность и содержание этапов разработки автоматизированных систем и подсистем безопасности автоматизированных систем, средства автоматизации проектирования автоматизированных систем; (ПК-20 .С3.Б19.1З) – методы и модели анализа угроз безопасности подсистем автоматизированных систем; методы, способы и средства обеспечения отказоустойчивости автоматизированных систем; (ПК-20 .С3.Б19.2З)	Лекции Семинарские занятия Самостоятельная работа студентов по изучению теоретического материала	Вопросы текущего, рубежного и итогового контроля; собеседование по самостоятельно изученному материалу
умеет: – выполнять работы по эксплуатации компонентов автоматизированных систем на объектах информатизации; (ПК-20 .С3.Б19.1У)	Практические занятия; выполнение индивидуального задания по тематике практических занятий	Темы индивидуального задания по тематике практических занятий
владеет: – программным обеспечением, предназначенным для автоматизированного исследования подсистем безопасности информационных систем. (ПК-20 .С3.Б19.1В)	Самостоятельная работа по индивидуальному заданию по учебному модулю дисциплины	Те мы индивидуальных заданий по учебному модулю дисциплины

3. Объем дисциплины и виды учебной работы

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

3.2. Основными видами аудиторной работы по дисциплине являются:

- лекции (ЛК);
- лабораторные работы
- практические занятия (ПЗ)
- семинарские занятия (СЗ).

3.3. Основными видами самостоятельной работы по дисциплине являются:

- самостоятельное изучение теоретического материала (ИТМ);
- выполнение индивидуальных заданий по тематике практических занятий (ИЗ);
- выполнение курсовой работы и защита отчета (КР).

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

Таблица 3.1 – Объём и виды учебной работы

№ п/п	Виды учебной работы	Трудоемкость в АЧ			Форма представления результатов
		8	9	Всего	
1	2	3	4	5	6
1	**Аудиторная работа:**	**63**	**90**	**153**	
	– в том числе в интерактивной форме	14	14	28	
	– лекции (Л)	16	32	48	конспект лекций
	– в том числе в интерактивной форме	4	4	8	
	– лабораторные работы	27	36	63	отчет о выполнении
	– практические занятия (ПЗ), семинарские занятия (СЗ)	18	18	36	отчет о выполнении
	– в том числе в интерактивной форме	10	10	20	
2	Контроль самостоятельной работы (КСР)	2	4	6	
3	**Самостоятельная работа студентов (СРС)**	**81**	**90**	**171**	
	Самостоятельное изучение теоретического материала (ИТМ)	20	50	70	отчет по вопросам для текущего и рубежного контроля
	Выполнение индивидуальных заданий по тематике практических занятий (ИЗ)	40	40	80	отчёт о выполнении
	Выполнение курсовой работы	21			отчёт о выполнении
4	Итоговая аттестация по дисциплине:	зачет	36	36	**Экзамен**
3	**Трудоемкость дисциплины, всего:** **в часах (АЧ)** **в зачетных единицах (ЗЕТ)**	**144** **4**	**216** **6**	**360** **10**	

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	ЛР	ПЗ, СЗ	КСР	Всего	ИТМ	ИЗ	КР		
1	2	3	4	5	6	7	8	9	10	11	12	13	14
1	1	1.1	2	2									2
		1.2	6	2		4		20	10	10			26
		1.3	8	4		4		10		10			18
	Всего по модулю:		**16**	8		8		**30**	10	20			**46**
2	1	1.4	10	2	8			7			7		17
		1.5	16	3	8	5		27	10	10	7		43
		1.6	21	3	11	5	2	17		10	7		38
	Всего по модулю:		**47**	8	27	10	2	**51**	10	20			**98**
Всего по разделу:			**63**	**16**	**27**	**18**	**2**	**81**	**20**	**40**	**21**		**144/4**
3	2	2.1	4	4				10	10				14
		2.2	10	6		4		20	10	10			30
		2.3	10	6		4		10		10			20
	Всего по модулю:		**24**	16		8		**40**	20	20			**64**
4	2	2.4	16	4	12			10	10				**26**
		2.5	23	6	12	5		30	20	10			**53**
		2.6	27	6	12	5	4	10		10			**37**
	Всего по модулю:		**66**	16	36	10	4	**50**	30	20			**116**
Всего по разделу:			**90**	**32**	**36**	**18**	**4**	**90**	**50**	**40**			**180/5**
Итоговая аттестация												**36**	**36/1**
Итого			**153**	**48**	**63**	**36**	**6**	**171**	**70**	**80**	**21**	**36**	**360/1**

4.2. Содержание разделов и тем учебной дисциплины

Раздел I. Безопасность информационных систем

Модуль 1. Безопасность информационных систем АРС: Л - 8 ч.; ПЗ (СЗ) - 8 ч., СРС: ИТМ - 10 ч., ИЗ - 20 ч.

Тема 1.1. Актуальность информационной безопасности, понятия и определения
Место информационной безопасности экономических систем в национальной безопасности страны. Концепция информационной безопасности. Международные стандарты информационного обмена. Классификация компьютерных преступлений. Способы совершения компьютерных преступлений. Пользователи и злоумышленники в Internet. Причины уязвимости сети Internet. Понятия и определения в информационной безопасности.

Тема 1.2. Угрозы информации
Виды угроз информационной безопасности. Три вида возможных нарушений информационной системы. Защита. Источники угроз информационной безопасности РФ. Информационная безопасность в условиях функционирования в России глобальных сетей. Виды противников или «нарушителей». Удаленные атаки на интрасети.

Тема 1.3. Критерии безопасности компьютерных систем
Стандарты безопасности. Критерии безопасности компьютерных систем «Оранжевая книга». Руководящие документы Гостехкомиссии.

Модуль 2. Методы обеспечения безопасности информационных систем АРС: Л - 8 ч.; ПЗ (СЗ) - 10 ч., ЛР – 27ч. СРС: ИТМ - 10 ч., ИЗ - 20 ч., КР – 21ч.

Тема 1.4. Безопасность информационных систем
Основные положения теории информационной безопасности информационных систем. Концепция информационной безопасности. Модели безопасности и их применение. Таксономия нарушений информационной безопасности вычислительной системы и причины, обуславливающие их существование. Анализ способов нарушений информационной безопасности. Использование защищенных компьютерных систем.

Тема 1.5. Методы и средства защиты компьютерной информации
Методы обеспечения информационной безопасности РФ. Ограничение доступа. Контроль доступа к аппаратуре. Разграничение и контроль доступа к информации. Предоставление привилегий на доступ. Идентификация и установление подлинности объекта (субъекта). Защита информации от утечки за счет побочного электромагнитного излучения и наводок. Методы и средства защиты информации от случайных воздействий. Методы защиты информации от аварийных ситуаций. Организационные мероприятия по защите информации. Организация информационной безопасности компании. Выбор средств информационной информации. Информационное страхование.

Тема 1.6. Лицензирование и сертификация в области защиты информации
Законодательство в области лицензирования и сертификации. Правила функционирования системы лицензирования. Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы. Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства.

Раздел II. Программные методы обеспечение информационной безопасности

Модуль 3. Методы обеспечения безопасности операционных систем и баз данных. АРС: Л - 16 ч; ПЗ (СЗ) - 8 ч., СРС: ИТМ - 20 ч., ИЗ - 20 ч.

Тема 2.1. Структура подсистем безопасности операционных систем
Архитектура операционных систем. Процесс загрузки операционных систем. Классификиция программного обеспечения. Защищенный режим работы процессора. Уровни доступа. Разграничение адресного пространства и ресурсов ПК. Драйверы. Сервисы. Утилиты.
Тема 2.2. Криптографические методы информационной безопасности
Методы криптографии. Классификация криптографических методов. Характеристики существующих шифров. Кодирование. Стеганография. Электронная цифровая подпись. Программные интерфейсы Crypto API.
Тема 2.3. Вредоносные программы
Условия существования вредоносных программ. Понятия о видах вирусов. Классические компьютерные вирусы. Сетевые черви. Троянские программы. Rootkit. Спам. Защита от компьютерных вирусов. Признаки заражения компьютера. Источники компьютерных вирусов. Основные правила защиты. Антивирусные программы

Модуль 4. Принципы разработки защищенного программного обеспечения.
АРС: Л - 16 ч; ПЗ (СЗ) - 10 ч., ЛР – 36ч. СРС: ИТМ - 30 ч., ИЗ - 20 ч.

Тема 2.4. Безопасность баз данных
Виды угроз. SQL Injection и XSS в распределенных информационных системах. Резервное копирование и восстановление данных. Разграничение доступа пользователей. Права доступа в БД. Использование процедур PL/SQL для повышения безопасности и быстродействия информационных систем. Аудит в БД. Повышение надежности систем хранения данных. Сериализация транзакций. Журнализация.
Тема 2.5. Безопасность операционных систем
Виды угроз. Разграничение доступа к ресурсам ИС. Идентификация и аутентификация пользователей в ОС семейства Windows и Linux. Аудит событий безопасности. Администрирование прав пользователей. Аппаратно-программные комплексы обеспечения безопасности ОС.
Тема 2.6. Разработка защищенных приложений
Управление доступом к ресурсам в программном коде. Получение информации об идентификации и аутентификации пользователей в ОС семейства Windows и Linux. Использование встроенных API шифрования Crypto API. Исследование программного кода для работы с электронными ключами.

4.3 Перечень тем практических занятий (семинаров)

Таблица 4.2 – Темы, практических занятий (ПЗ)

№ п/п	Номер темы дисциплины	Наименование темы практического занятия	Тр.ч
1	1.2	Информационные отношения как объект правового регулирования; Правовой режим защиты государственной тайны; Правовой режим защиты информации конфиденциального характера	4
2	1.3	Организация многорубежной системы охраны; Организация режимных мероприятий	4
3	1.5	Институт правовой защиты служебной тайны; Институт правовой защиты коммерческой тайны; Институт правовой защиты банковской тайны; Допуск к государственной тайне. Организация служебного расследования по фактам утраты информации	5
4	1.6	Модель угроз. Модель нарушителя. Классы информационных систем	5
5	2.2	Понятие и сущность программной защиты информации. Управление правами пользователей. Локальная политика безопасности в	4

		Windows и Linux	
6	2.3	Вирусы. Руткиты. Антивирусы. Архитектура и возможности программного обеспечения антивирусов. Интеграция в файловую и сетевую подсистемы.	4
11	2.5	Электронные ключи и смарт-карты для обеспечения разграничения доступа и шифрования.	5
12	2.6	Программные интерфейсы и библиотеки криптопровайдеров Crypto API.	5
		Всего:	36/1

4.4 Перечень тем лабораторных работ

Таблица 4.4 – Темы лабораторных работ (ЛР)

№ п/п	Номер темы дисциплины	Наименование темы практического занятия (семинара)	Тр.ч
1	1.4	Локальная безопасность Windows и анализ уязвимостей операционной системы	4
2	1.4	Локальная безопасность Linux и анализ уязвимостей операционной системы	4
3	1.5	Использование программного обеспечения шифрования данных. Использование безопасных протоколов передачи данных. Перехват трафика с использованием ПО Wireshark	8
4	1.6	Модели безопасности ИС и их применение	3
5	1.6	Централизованная настройка информационной безопасности Windows Active Directory и интеграция Samba Server в AD	8
6	2.4	Настройка типового антивируса. Обновление баз. Настройка файервола. Поиск вирусной активности с использованием реестра, диспетчера процессов, файловых менеджеров	4
7	2.4	Установка СУБД Oracle XE на подготовленной виртуальной машине. Настройка автоматического резервного копирования. Перенос данных с помощью утилит экспорта/импорта. Подключение к удаленным БД. СУБД Oracle XE: Создание пользователей и задание привилегий. Создание пакетов процедур и триггеров на языке PL/SQL. Настройка аудита	6
8	2.5	Настройка виртуальной машины Virtual PC. Поиск уязвимостей сканерами безопасности. Настройка локальной политики безопасности и аудита. Установка прав на доступ к файловым объектам, реестру и журналам событий. Использование Kali Linux для реализации атак и закрытие уязвимостей	12
9	2.6	Разработка приложения для работы с БД, исследование прав пользователей БД	6
10	2.6	Разработка приложения для работы с электронными ключами	6
		Всего:	63/1.8

4.5 Виды самостоятельной работы студентов

По каждому практическому занятию студентам выдается индивидуальное задание, в рамках которого необходимо решить задачу, сформулированную по рассмотренной тематике. Перечень типовых задач приводится в методических указаниях к проведению практических занятий.

По индивидуальному заданию по курсовой работе студент должен оформить и защитить отчет, в котором приводятся описание среды реализации, краткие сведения из теории, основные этапы работы, представление результатов выполнения индивидуального задания и выводы.

Собеседование по тематике самостоятельно изученного теоретического материала определяет уровень проработки перечня вопросов, рассматриваемых в рамках соответствующей темы, выделенной на аудиторное или самостоятельное изучение.

Перечень отчетных документов, подготовленных студентом при выполнении индивидуальных видов СРС:

– отчетов по выполнению индивидуального задания по тематике практических занятий – 6 (ИЗ1 – ИЗ6);

– отчет по выполнению курсовой работы – КР;

Форма представления результатов изучения – собеседование.

Таблица 4.5 – Виды самостоятельной работы студентов (СРС)

Номер темы (раздела) дисциплины	**Вид самостоятельной работы студентов**	**Трудоёмкость, часов**
1	2	3
1.2	ИТМ: Перспективы развития законодательства в области информационной безопасности; ИТМ: Правовая регламентация сертификационной деятельности в области обеспечения информационной безопасности. Органы сертификации и их полномочия	10
1.5	ИТМ: Режим защиты информации как составная часть организационной защиты информации ; Практика расследования преступлений в сфере компьютерной информации	10
2.2	ИТМ: Архитектура операционной системы Linux и принципы разграничения ресурсов и многопользовательской работы.	10
1.5	ИЗМ: Система шифрования Континент. Использование крипто-шлюза для организации информационного обмена в сетях общего пользования	10
	Итого: в **ч** / в **ЗЕ**	**40/1,1**

4.5.1. Темы для выполнения индивидуального задания по тематике практических занятий (ИЗ)

Раздел 1, модули 1,2.

1. Проблемы применения норм права для пресечения компьютерной преступности на международном и внутригосударственном уровне.
2. Области взаимодействия частных охранных предприятий с государственными правоохранительными органами.
3. Правовое обеспечение защиты негосударственных объектов экономики.
4. Состояние и перспективы правовой защиты интеллектуальной собственности в России и за рубежом.
5. Деятельность организаций, выполняющих контролирующие и правоохранительные функции в РФ в области защиты интеллектуальной собственности.
6. Практика применения нормативно-правовой базы лицензирования и сертификации в области защиты государственной тайны в РФ.

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

8. Перспективы развития правовой защиты профессиональной тайны.

9. Порядок и регулирование вопросов международного обмена конфиденциальной информацией.

10. Опыт применения российских и международных стандартов безопасности.

11. Правовая защита информационных технологий против компьютерных преступлений.

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

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

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

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

16. Правовое регулирование защиты персональных данных в России и за рубежом.

17. Правовое регулирование использования специальных технических средств получения и защиты информации.

Раздел 2, модули 3,4.

18. Настройка типового антивируса. Обновление баз. Настройка файервола.

19. Поиск вирусной активности с использованием реестра, диспетчера процессов, файловых менеджеров

20. Установка СУБД Oracle XE на подготовленной виртуальной машине.

21. Настройка автоматического резервного копирования.

22. Перенос данных с помощью утилит экспорта/импорта.

23. Подключение к удаленным БД.

24. СУБД Oracle XE: Создание пользователей и задание привилегий.

25. Создание пакетов процедур и триггеров на языке PL/SQL. Настройка аудита

26. Настройка виртуальной машины Virtual PC. Поиск уязвимостей сканерами безопасности.

27. Настройка локальной политики безопасности и аудита.

28. Установка прав на доступ к файловым объектам, реестру и журналам событий.

29. Использование Kali Linux для реализации атак и закрытие уязвимостей

30. Разработка приложения для работы с БД, исследование прав пользователей БД

31. Разработка приложения для работы с электронными ключами.

4.5.2 Перечень тем курсовых работ (проектов)

4.7. Типовая тема курсовой работы

1. Типовая тема курсовой работы по дисциплине:

Разработка клиент-серверного программного обеспечения для заданной предметной области.

2. Цель курсовой работы по дисциплине:

– освоение методов проектирования автоматизированных информационных систем;

– освоение языка SQL;

– освоение основ программирования на языке C#;

– исследование возможностей интеграции интерфейсов CryptoAPI в ПО;

– управление доступом к объектам реестра и файлам средствами C#.

3. Результаты выполнения курсовой работы по дисциплине:

– должна быть разработана модель ИУС, модель базы данных, разработаны диаграммы IDEF, ERD, DFD;

– должны быть разработаны командные последовательности на языке SQL для создания схемы данных в БД.

– должно быть разработано программное обеспечение для работы с БД

– должно быть реализовано взимодействие двух программ с использованием сгенерированных ключей, состоящее из процедуры обмена ключами и процедуры обмена зашифрованными данными

– должно быть реализовано сохранение настроек ПО в реестре и в файловой системе и защита веток реестра от несанкционированного изменения.

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

6 Управление и контроль освоения компетенций

6.1 Текущий контроль освоения заданных дисциплинарных компетенций

Текущий контроль освоения дисциплинарных компетенций проводится в следующих формах:

– текущий опрос, текущая проверочная работа для анализа усвоения материала предыдущей лекции;

– оценка работы студента на лекционных, практических 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 по курсовой работе (модуль 2);

– отчеты по лабораторным работам (модуль 1, 2, 3,4).

– отчеты по индивидуальным заданиям к практическим занятиям (модуль 1, 2, 3,4).

– вопросы для рубежного контроля (модуль 1, 2, 3,4).

6.3 Итоговый контроль освоения заданных дисциплинарных компетенций

1) **Зачёт (8-й семестр)**

2) **Экзамен (9-й семестр)**

Итоговый контроль уровня освоения заданных дисциплинарных компетенции производится в виде зачета (8сем.) и экзамена(9сем.). Допуск к зачету и экзамену по дисциплине предоставляется по итогам проведения рубежного контроля по выполнению всех индивидуальных заданий по модулю, результатам практических и семинарских занятий.

Зачет и экзамен по дисциплине проводится устно по билетам. Билет содержит два теоретических вопроса по программно-аппаратному обеспечению информационной безопасности, в зависимости от раздела изучения дисциплины.

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

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

Таблица 6.4. Структура учебной работы студента по видам, формам представления результатов и формам контроля

Коды компонентов ДК	Компоненты ДК	Формулировки компонентов ДК	АРС		СРС		№ Темы
			Форма выполнения	Форма контроля	Форма представления результатов	Форма контроля	
ПК-14 .С3.Б19	Знает:	модели данных, систем и процессов защиты информации в автоматизированных системах, критерии оценки защищенности автоматизированных систем; (1з)	ЛК7 С3	Текущий, промежут.	ИТМ3	Собеседование, защита	1.5
		основные угрозы безопасности информации и модели нарушителя в автоматизированных системах (2з)	ЛК4, ЛК6, ПЗ2	Текущий, промежут.	ИТМ4 ИЗ2	Собеседование, защита	1.4 1.5 1.6
	Умеет:	определять комплекс мер для обеспечения информационной безопасности автоматизированных систем (1у);	ПЗ3 ЛР1 ЛР2 ЛР3	Рубежный	ИЗ3	Защита	1.3
	Владеет:	методами и технологиями проектирования, моделирования, исследования подсистем безопасности автоматизированных систем (1в).	КР	Рубежный	КР	Защита	1.4 1.5 1.6
ПК-13 .С3.Б19	Знает:	содержание и порядок деятельности персонала по эксплуатации защи-	ЛК2 ЛК3 ПЗ3	Текущий, промежут.	ИТМ1 ИЗ3	Собеседование, защита	1.1 1.2 1.3

		щенных автоматизированных систем и подсистем безопасности автоматизированных систем (1з);	ПЗ4		ИЗ4		
		информации в автоматизированных системах, состав работ по защите информации на стадиях и этапах создания автоматизированных систем, с учетом требований нормативно-технической документации; (2з);	ЛК4, ЛК5 ПЗ6	Текущий, промежут.	ИТМ3 ИЗ6	Собеседд., защита	1.5 1.6
	Умеет:	определять комплекс мер для обеспечения информационной безопасности автоматизированных систем (1у);	ПЗ1 ЛР4 ЛР5 ЛР6	Рубежный	ИЗ1	Защита	1.2 1.5 1.6
		выполнять работы по эксплуатации компонентов автоматизированных систем на объектах информатизации (2у);	ПЗ3 ПЗ4 ПЗ5 ПЗ6 ПЗ7	Рубежный	ИЗ2 ИЗ4 ИЗ5	Защита Защита	2.3 2.4 2.5 2.6
	Владеет:	методами и технологиями проектирования, моделирования, исследования подсистем безопасности автоматизированных систем (1в).			КР	Защита	1.6
ПК-20 .С3.Б19	Знает:	методы, способы, средства, последовательность и содержание этапов разработки автоматизированных систем и подсистем безопасности автоматизированных систем, средства автоматизации проектирования автоматизированных систем; (1з);	ЛК9 ЛК10 ПЗ5 ПЗ6	Текущий, промежут.	ИТМ3 ИЗ3 ИЗ4	Собеседд. защита	2.1 2.2 2.3
		методы и модели анализа угроз безопасности подсистем автоматизированных систем; методы, способы и средства обеспечения отказоустойчивости автоматизированных систем; (2з);	ЛК11, ЛК12 ПЗ7 ПЗ8	Текущий, промежут.	ИТМ4 ИЗ7 ИЗ8	Собеседд., защита	2.5 2.6
	Умеет:	выполнять работы по эксплуатации компонентов автоматизированных систем на объектах информатизации (1у);	ПЗ8 ЛР8 ЛР9 ЛР10	Рубежный	ИЗ8	Защита	2.2 2.5 2.6

	Владеет:	программным обеспечением, предназначенным для автоматизированного исследования подсистем безопасности информационных систем (1в).			КР	Защита	1.5

7 График учебного процесса по дисциплине

Таблица 7.1 – График учебного процесса по дисциплине (М1-2)

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:	**Р1**																		
Лекции	2	2	2				2	2	2	2	2		2	2	2	2			**16**
Практические, семинарские занятия (ПЗ, СЗ)			2	2	2	2		2	2	2	2		2	2	2	2			**18**
Самост. изучение теоретического материала		2	2		2	2	2	2			2	2	2		2	2	2		**20**
Лабораторные работы (ЛР)										4	4	4	4	4	4	3			**27**
Вып. Курсовой работы (КР)										2	2	2	2	2	4	4	3		**21**
КСР																	2		**2**
Модуль:	**1**						**2**						**3**						
Контр. тестирование						+					+							+	
Дисциплин. контроль																			**зачет.**

Продолжение таблицы 7.1 – График учебного процесса по дисциплине (М3-4)

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:	**Р2**																		
Лекции	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	**32**
Практические, семинарские занятия (ПЗ, СЗ)					2	2	2		2	2			2	2	2	2			**18**
Самост. изучение теоретического материала		2		2	2		2	2	2		2	2		2	2				**20**
Лабораторные работы (ЛР)										4	4	4	4	4	4	4	4	4	**36**
КСР									2								2		**4**
Модуль:	**1**						**2**						**3**						
Контр. тестирование						+					+							+	
Дисциплин. контроль																			**Экз.**

8. Учебно-методическое и информационное обеспечение дисциплины

8.1. Карта обеспеченности дисциплины учебно-методической литературой

Безопасность операционных систем	*Профессиональный цикл*	
полное название дисциплины	[x] основная [ ] по выбору студента	[x] базовая часть цикла [ ] вариативная часть цикла

09030307.65	**«Информационная безопасность автоматизированных систем»,** специализация «Обеспечение информационной безопасности распределенных информационных систем»
код направления / специальности	*полное название направления/ специальности*

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

2015 семестр (ы) 8,9 количество групп **1**
количество студентов **20**

Кокоулин Андрей Николаевич, 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, 2008,2009.— 415 с.	12
2	Голенищев Э.П. Информационное обеспечение систем управления: учеб. пособие для вузов – Ростов-на-Дону : Феникс, 2010. – 315 с. : ил..	5
3	Громов Ю.Ю. Информационная безопасность и защита информации : учебное пособие для вузов / Ю. Ю. Громов [и др.] .— Старый Оскол : ТНТ, 2010 .— 383 с. : ил	5
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	Бабаш А.В. Информационная безопасность. Лабораторный практикум : учебное пособие для вузов / А. В. Бабаш, Е. К. Баранова, Ю. Н. Мельников .— Москва : КНОРУС, 2012 .— 131 с., 8,5 усл. печ. л. : ил. + CD-ROM .	2
2	Т.Кайт. Oracle для профессионалов : пер. с англ. / Том Кайт. Кн. 1: Архитектура и основные особенности .— 2-е изд. — 2004 .— 662 с	3
3	Т.Кайт. Oracle для профессионалов / Том Кайт Кн.2: Расширение возможностей и защита .— 2-е изд. — 2004 .— 831 с	3

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

8.3 Программные инструментальные средства

Не предусмотрены

8.4 Аудио- и видео-пособия

Не предусмотрены

9 Материально-техническое обеспечение дисциплины

9.1 Специализированные лаборатории и классы

Таблица 9.1 – Специализированные лаборатории и классы

№ п.п.	Помещения			Площадь, $м^2$	Количество посадочных мест
	Название	Принадлежность (кафедра)	Номер аудитории		
1	Дисплейный класс	Кафедра АТ	321 корп. А	34	18

9.2 Основное учебное оборудование

Таблица 9.2 – Учебное оборудование

№ п.п.	Наименование и марка оборудования (стенда, макета, плаката)	Кол-во, ед.	Форма приобретения / владения (собственность, оперативное управление, аренда и т.п.)	Номер аудитории
1	ПК Intel Pentium Dual CPU 2000 МГц	12	Оперативное управление	321 корп. А

Лист регистрации изменений

№ п.п.	Содержание изменения	Дата, номер протокола заседания кафедры
1.		
2.		
3.		
4.		
5.		

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
«Безопасность операционных систем»
РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Специальность:	10.05.03 Информационная безопасность автоматизированных систем
Специализация:	Обеспечение информационной безопасности распределенных информационных систем
Квалификация выпускника:	специалист
Выпускающая кафедра:	Автоматика и телемеханика
Форма обучения:	очная

Курсы: 4,5 Семестры: 8,9

Трудоемкость:

Кредитов по рабочему учебному плану (БУП): **10**
Часов по рабочему учебному плану (БУП): **360**

Виды контроля:
Экзамен: **- 9** Зачет: **- 8** Курсовой проект: **- нет** Курсовая работа: **- 8**

Пермь 2017 г.

Рабочая программа дисциплины «Безопасность операционных систем» разработана на основании:

- Федерального государственного образовательного стандарта высшего образования по специальности 10.05.03 Информационная безопасность автоматизированных систем (уровень специалитета), утвержденного приказом Министерства образования и науки Российской Федерации от «01» декабря 2016 г. № 1509;
- Компетентностной модели выпускника образовательной программы высшего образования – программы по специальности 10.05.03 Информационная безопасность автоматизированных систем, специализации «Обеспечение информационной безопасности распределенных информационных систем», утвержденной «24» июня 2013 г. (с изменениями, в связи с переходом на ФГОС ВО);
- Базового учебного плана очной формы обучения образовательной программы высшего образования – программы по специальности 10.05.03 Информационная безопасность автоматизированных систем, специализации «Обеспечение информационной безопасности распределенных информационных систем», утвержденного «22» декабря 2016 г.

Рабочая программа согласована с рабочими программами дисциплин, участвующих в формировании компетенций и их составляющих, приобретение которых является целью данной дисциплины:

Основы построения инфокоммуникационных систем и сетей, Научно-исследовательская работа студента, Метрология, стандартизация и сертификация базового учебного плана образовательной программы высшего образования - программы по специальности 10.05.03 Информационная безопасность автоматизированных систем, специализации Обеспечение информационной безопасности распределенных информационных систем.

Лист регистрации изменений

№ п.п	Содержание изменения	Дата, номер протокола заседания кафедры. Подпись заведующего кафедрой
1.	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 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 считать профессиональную компетенцией ПК-5 с формулировкой: «Способность разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированных систем»; - изменить шифр дисциплинарной компетенции с ПК-13.С3.Б19 на ПК-5.Б1.Б.36; - профессиональную компетенцию ПК-14 считать профессиональной компетенцией ПК-4 с формулировкой «Способность проводить анализ рисков информационной безопасности автоматизированных систем»; - изменить шифр дисциплинарной компетенции с ПК-14.С3.Б19 на ПК-9.Б1.Б.36; - профессиональную компетенцию ПК-21 считать профессиональной компетенцией ПСК-7.4 с формулировкой «Способность разрабатывать политики информационной безопасности автоматизированных систем»; - изменить шифр дисциплинарной компетенции с ПК-21.С3.Б19 на ПСК-7.4.Б1.Б.36;	
	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 10 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. Пере-	

	чень 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.		