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.т.н., проф.
_____ Н. В. Лобов
«___» _____ 2014 г.

УНИФИЦИРОВАНЫЙ УЧЕБНО-МЕТОДИЧЕСКИЙ КОМПЛЕКС ДИСЦИПЛИНЫ
«Основы информационной безопасности»

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: 2 **Семестр:** 4

Трудоёмкость:
Кредитов по рабочему учебному плану: 4 ЗЕТ
Часов по рабочему учебному плану: 144 АЧ

Виды контроля:
Экзамен: 4

Пермь 2014 г.

Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
**«Пермский национальный исследовательский
политехнический университет»**
Электротехнический факультет
Кафедра «Автоматика и телемеханика»

УТВЕРЖДАЮ
Заведующий кафедрой
«Автоматика и телемеханика»
д-р техн. наук, проф.
_____ А.А. Южаков
Протокол заседания кафедры АТ
от «16» января 2017 г. № 18

УЧЕБНО-МЕТОДИЧЕСКИЙ КОМПЛЕКС ДИСЦИПЛИНЫ
«Основы информационной безопасности»
РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

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

Курс: 2 **Семестр:** 4

Трудоемкость:

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

Виды контроля:

Экзамен: **- 4** Зачет: **- нет** Курсовой проект: **- нет** Курсовая работа: **- нет**

Пермь 2017 г.

Рабочая программа дисциплины «Основы информационной безопасности» разработана на основании:

- Федерального государственного образовательного стандарта высшего профессионального образования утвержденного приказом Министерства образования и науки Российской Федерации «17» января 2011 г. № 60, по направлению подготовки (специальности) 090303 «Информационная безопасность автоматизированных систем» (квалификация (степень) «специалист»);
- Федерального государственного образовательного стандарта высшего профессионального образования, утвержденного приказом Министерства образования и науки Российской Федерации от «28» октября 2009 г., № 496, по направлению подготовки 090900 Информационная безопасность (квалификация (степень) «бакалавр»);
- Компетентностной модели (КМ) выпускника ООП по профилю подготовки 090900.03.62 - Информационная безопасность, утвержденной «24» июня 2013 г.;
- Компетентностной модели (КМ) выпускника ООП по специализации подготовки 090303.07.65 - Обеспечение информационной безопасности распределенных информационных систем, утвержденной«24» июня 2014 г.;
- Рабочего учебного плана очной формы обучения по профилю подготовки 090900.03.62 - Информационная безопасность, (набор 2011 года), утвержденного «07» июня 2011 г.
- Рабочего учебного плана очной формы обучения по специализации подготовки 090303.07.65 - Обеспечение информационной безопасности распределенных информационных систем, (набор 2011 года), утвержденного «29» августа 2011 г.

Рабочая программа согласована с рабочей программой дисциплин: Введение в специальность, Организационное и правовое обеспечение информационной безопасности, Разработка и эксплуатация защищенных автоматизированных систем.

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

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

Рабочая программа рассмотрена и одобрена на заседании кафедры «Автоматика и телемеханика» «26» марта 2013 г., протокол № 26
Заведующий кафедрой,
«Автоматика и телемеханика»,
д-р. техн. наук, профессор _____ Южаков А.А.

Рабочая программа одобрена методической комиссией электротехнического факультета
«5» 04 2013 г., протокол № 5
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 «Основы информационной безопасности» разработана на основании:

- Федерального государственного образовательного стандарта высшего образования по направлению подготовки 10.03.01 Информационная безопасность (уровень бакалавриата), утвержденного приказом Министерства образования и науки Российской Федерации от «01» декабря 2016 г. № 1515;
- Федерального государственного образовательного стандарта высшего образования по специальности 10.05.03 Информационная безопасность автоматизированных систем (уровень специалитета), утвержденного приказом Министерства образования и науки Российской Федерации от «01» декабря 2016 г. № 1509;
- Компетентностной модели выпускника образовательной программы высшего образования – программы бакалавриата по направлению подготовки 10.03.01 Информационная безопасность направленности (профиля) «Комплексная защита объектов информатизации», утвержденной «24» июня 2013 г. (с изменениями, в связи с переходом на ФГОС ВО);
- Компетентностной модели выпускника образовательной программы высшего образования – программы по специальности 10.05.03 Информационная безопасность автоматизированных систем, специализации «Обеспечение информационной безопасности распределенных информационных систем», утвержденной «24» июня 2013 г. (с изменениями, в связи с переходом на ФГОС ВО);
- Базового учебного плана очной формы обучения образовательной программы высшего образования – программы бакалавриата по направлению подготовки 10.03.01 Информационная безопасность, направленности (профиля) «Комплексная защита объектов информатизации», утвержденного «22» декабря 2016 г.
- Базового учебного плана очной формы обучения образовательной программы высшего образования – программы по специальности 10.05.03 Информационная безопасность автоматизированных систем, специализации «Обеспечение информационной безопасности распределенных информационных систем», утвержденного «22» декабря 2016 г.

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

Социология и политология, История защиты информации, Введение в специальность, Основы построения инфокоммуникационных систем и сетей, Документоведение, Научно-исследовательская работа студентов базового учебного плана образовательной программы высшего образования - программы бакалавриата по направлению 10.03.01 Информационная безопасность, направленности (профиля) Комплексная защита объектов информатизации;

Социология и политология, 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.

1. Общие положения

1.1. Цель дисциплины - изучение принципов обеспечения информационной безопасности государства, подходов к анализу угроз его информационной инфраструктуры и освоение дисциплинарных компетенций для решения задач защиты информации в информационных системах, а также формирование фундаментальных знаний в области информационной безопасности.

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

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

№	Код направления/ специальности	Наименование направления/ специальности	Компетенции, формируемые на основе базовых учебных планов	
			Код компетенции	Формулировка компетенции
1.	090900.62	Информационная безопасность	ОК-7	способность осознавать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности, готовностью и способностью к активной состязательной деятельности в условиях информационного противоборства
			ПК-24	способность осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов по вопросам обеспечения информационной безопасности
2.	090303.65		ОК-5	способность понимать социальную значимость своей будущей профессии, цели и смысл государственной службы, обладать высокой мотивацией к профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, готовностью и способностью к активной состязательной деятельности в условиях информационного противоборства
			ПК-9	способность осуществлять поиск, изучение, обобщение и систематизацию научно-технической информации, нормативных и методических материалов в сфере своей профессиональной деятельности

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

Унифицированная общекультурная компетенция (УОК-1)

Способность осознавать и понимать социальную значимость своей будущей профессии, цели и смысл государственной службы, обладать высокой мотивацией к профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, готовностью и способностью к активной состязательной деятельности в условиях информационного противоборства

Унифицированная профессиональная компетенция (УПК-1)

Способность осуществлять подбор, изучение, обобщение и систематизацию научно-технической информации, научно-технической литературы, нормативных и методических материалов по вопросам обеспечения информационной безопасности в сфере своей профессиональной деятельности

Таблица 1.2 Обоснование разработки унифицированных компетенций

№	Направление подготовки		Соответствие унифицированной компетенции и базовой компетенции ФГОС ВПО	
	Код	Наименование	**Способность осознавать и понимать социальную значимость своей будущей профессии, цели и смысл государственной службы, обладать высокой мотивацией к профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, готовностью и способностью к активной состязательной деятельности в условиях информационного противоборства (УОК-1)**	**Способность осуществлять подбор, изучение, обобщение и систематизацию научно-технической информации, научно-технической литературы, нормативных и методических материалов по вопросам обеспечения информационной безопасности в сфере своей профессиональной деятельности (УПК-1)**
1.	090900.62	Информационная безопасность	способность осознавать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности, готовностью и способностью к активной состязательной деятельности в условиях информационного противоборства (ОК-7)	способность осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов по вопросам обеспечения информационной безопасности (ПК-24)

1	2	3	4	5
2.	090303.65	Информационная безопасность автоматизированных систем	способностью понимать социальную значимость своей будущей профессии, цели и смысл государственной службы, обладать высокой мотивацией к профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, готовностью и способностью к активной состязательной деятельности в условиях информационного противоборства (ОК-5)	способность осуществлять поиск, изучение, обобщение и систематизацию научно-технической информации, нормативных и методических материалов в сфере своей профессиональной деятельности (ПК-9)

1.2. Задачи дисциплины:

– изучение основных положений государственной политики в области обеспечения информационной безопасности Российской Федерации, основных понятий в области защиты информации и методологических принципов создания систем защиты информации;

– изучение видов защищаемой информации, угроз информационной безопасности, сущности и разновидностей информационного оружия, методов и средств ведения информационных войн;

– изучение методов и средств обеспечения информационной безопасности компьютерных систем, механизмов защиты информации, формальных моделей безопасности, критериев оценки защищенности и обеспечения безопасности автоматизированных систем;

– приобретение умений в подборе и анализе показателей качества и критериев оценки систем безопасности, отдельных методов и средств защиты информации, использовании современной научно-технической литературой для решения задач по вопросам защиты информации;

– приобретение навыков анализа информационной инфраструктуры государства с точки зрения информационной безопасности, подбора нормативных и методических материалов по вопросам защиты информации.

После изучения дисциплины обучающийся должен демонстрировать следующие результаты:

знать:

- роль специалиста по защите информации, цели и смысл государственной службы, место информационной безопасности в системе национальной безопасности страны;
- угрозы информационной безопасности государства;
- содержание информационной войны, методы и средства ее ведения;
- виды информации ограниченного доступа, в соответствии с требованиями Российского законодательства;
- основные понятия в области информационной безопасности и методологические принципы создания систем защиты информации;

- методы и средства и обеспечения информационной безопасности компьютерных систем, механизмы защиты информации;
- критерии оценки защищенности автоматизированных систем и современные методы обеспечения их информационной безопасности;
- особенности обеспечения информационной безопасности автоматизированных систем при обработке информации, составляющей государственную тайну;

уметь:

- выбирать и анализировать показатели качества и критерии оценки систем и отдельных методов и средств защиты информации;
- подбирать информацию и пользоваться современной научно-технической литературой для решения задач защиты информации;

владеть:

- навыками активной состязательной деятельности в условиях информационного противоборства;
- навыками подбора нормативных и методических материалов по вопросам обеспечения информационной безопасности.

1.3. Предметом освоения дисциплины являются следующие объекты:

- понятие национальной безопасности;
- информационная безопасность в системе национальной безопасности Российской Федерации;
- государственная информационная политика;
- основные понятия, общеметодологические принципы теории информационной безопасности;
- анализ угроз информационной безопасности;
- проблемы информационных войн;
- проблемы региональной информационной безопасности;
- виды информации ограниченного доступа;
- методы нарушения конфиденциальности, целостности и доступности информации;
- причины, виды, каналы утечки и искажения информации;
- формальные модели безопасности;
- способы и средства обеспечения информационной безопасности;
- критерии оценки защищенности информационных систем.

1.4. Место дисциплины в структуре профессиональной подготовки выпускников

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

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

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

Таблица 1.3. – Дисциплины, направленные на формирование компетенций

Код	Наименование компетенций	Предшествующие дисциплины	Последующие дисциплины
УОК-1	Способность осознавать и понимать социальную значимость своей будущей профессии, цели и смысл государственной службы, обладать высокой мотивацией к профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, готовностью и способностью к активной состязательной деятельности в условиях информационного противоборства	Экономика Социология и политология Введение в специальность	Организационное и правовое обеспечение информационной безопасности Разработка и эксплуатация защищенных автоматизированных систем
УПК-1	Способность осуществлять подбор, изучение, обобщение и систематизацию научно-технической информации, научно-технической литературы, нормативных и методических материалов по вопросам обеспечения информационной безопасности в сфере своей профессиональной деятельности	Документоведение	Основы построения инфокоммуникационных систем и сетей Комплексная защита информации на предприятии

2. Требования к результатам освоения учебной дисциплины

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

2.1. Дисциплинарная карта компетенции УОК-1

Код УОК-1	**Формулировка унифицированной дисциплинарной компетенции** Способность осознавать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности, готовностью и способностью к активной состязательной деятельности в условиях информационного противоборства

Требования к компонентному составу компетенции

Перечень компонентов	Виды учебной работы	Средства оценки
Знает: – роль специалиста по защите информации, цели и смысл государственной службы, место информационной безопасности в системе национальной безопасности страны; – угрозы информационной безопасности государства; – содержание информационной войны, методы и средства ее ведения;	Лекции Семинарские занятия Самостоятельная работа студентов по изучению теоретического материала	Вопросы для текущего и рубежного контроля

Умеет: – анализировать информацию по вопросам национальной и информационной безопасности государства; – анализировать угрозы безопасности информационной инфраструктуры государства; – выбирать критерии оценки защищенности информационной инфраструктуры государства;	Практические занятия Самостоятельная работа студентов по решению практических задач Самостоятельная работа студентов по подготовке к экзамену	Отчет за выполнение практических заданий на ПЗ Отчёт по индивидуальным заданиям по модулю
Владеет: – навыками активной состязательной деятельности в условиях информационного противоборства	Самостоятельная работа студентов по решению практических задач Самостоятельная работа по подготовке к экзамену	Отчет за выполнение практических заданий на ПЗ Отчёт по индивидуальным заданиям по модулю

2.2. Дисциплинарная карта компетенции УПК-1

Код УПК-1	**Формулировка унифицированной дисциплинарной компетенции** Способность осуществлять подбор, изучение, обобщение и систематизацию научно-технической информации, научно-технической литературы, нормативных и методических материалов по вопросам обеспечения информационной безопасности в сфере своей профессиональной деятельности

Требования к компонентному составу компетенции

Перечень компонентов	Виды учебной работы	Средства оценки
Знает: – виды информации ограниченного доступа, основные понятия в области информационной безопасности и методологические принципы создания систем защиты информации; – методы, средства защиты информации, критерии оценки защищенности компьютерных систем;	Лекции Семинарские занятия Самостоятельная работа студентов по изучению теоретического материала	Вопросы для текущего и рубежного контроля
Умеет: – выбирать и анализировать показатели качества и критерии оценки систем и отдельных методов и средств защиты информации; – пользоваться современной научно-технической литературой для решения задач защиты информации;	Практические занятия Самостоятельная работа студентов по решению практических задач Самостоятельная работа студентов по подготовке к экзамену	Отчет за выполнение практических заданий на ПЗ Отчёт по индивидуальным заданиям по модулю

Владеет: – навыками подбора нормативных и методических материалов по вопросам обеспечения информационной безопасности	Самостоятельная работа студентов по решению практических задач Самостоятельная работа по подготовке к экзамену	Отчет за выполнение практических заданий на ПЗ Отчёт по индивидуальным заданиям по модулю

3. Объем дисциплины и виды учебной работы

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

3.2. Основными видами аудиторной работы по дисциплине являются:

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

3.3. Основными видами самостоятельной работы по дисциплине являются:

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

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

Таблица 3.1 – Объём и виды учебной работы

№ п.п.	Виды учебной работы	Трудоёмкость, ч	Форма представления результатов
1	2	3	4
1	**Аудиторная работа**	**52**	
	- 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)	**54**	
	- самостоятельное изучение теоретического материала (ИТМ)	24	отчет по вопросам для текущего и рубежного контроля
	- выполнение индивидуальных заданий по модулю (ИЗМ)	30	отчёт о выполнении
3	Итоговая аттестация по дисциплине:	**36**	**Экзамен**
4	**Трудоёмкость дисциплины, всего:** **в часах (ч)** **в зачётных единицах (ЗЕ)**	 **144** **4**	

4. Содержание учебной дисциплины

4.1. Модульный тематический план

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

Таблица 4.1 – Тематический план по модулям учебной дисциплины

Номер учебного модуля	Номер раздела дисциплины	Номер темы дисциплины	Количество часов (очная форма обучения)							Итог. аттест.	Трудоёмкость АЧ/ ЗЕТ
			Аудиторная работа студента (АРС)				Самостоятельная работа студента (СРС)				
			Всего	Лк	ПЗ, СЗ	КСР	Всего	ИТМ	ИЗМ		
1	2	3	4	5	6	7	8	9	10	11	12
1	1	1	4	2	2		2	2			6
		2	4	2	2		2	2			6
		3	4	2	2		2	2			6
		4	4	2	2		12	2	10		16
	Всего по модулю:		**16**	8	8		**18**	8	10		**34**
2	2	5	4	2	2		2	2			6
		6	4	2	2		2	2			6
		7	4	2	2		12	2	10		16
	Всего по модулю:		**12**	6	6		**16**	6	10		**28**
3	3	8	4	2	2		2	2			6
		9	4	2	2		2	2			6
		10	6	2	4		2	2			8
		11	6	2	4		2	2			8
		12	6	2	2	2	12	2	10		18
	Всего по модулю:		**26**	10	14	2	**20**	10	10		**46**
Итоговая аттестация										36	**36**
Итого			**54**	**24**	**28**	**2**	**54**	**24**	**30**	**36**	**144/4**

4.2. Содержание разделов и тем учебной дисциплины

Модуль 1. Информационная безопасность в системе национальной безопасности Российской Федерации

Раздел 1. Информационная безопасность в системе национальной безопасности Российской Федерации. АРС: Л - 8 ч, СЗ - 4×2 = 8 ч., СРС: ИТМ - 8 ч., ИЗМ (ИЗМ-1) - 10 ч.

Тема 1. Национальная безопасность Российской Федерации. Понятие национальной безопасности. Виды безопасности и сферы жизнедеятельности личности, общества и государства. Национальные интересы РФ и стратегические национальные приоритеты. Цели и смысл государственной службы. Роль специалиста по защите информационной безопасности в обеспечении национальной безопасности государства.

Тема 2. Основы государственной политики и угрозы безопасности Российской Федерации в информационной сфере.

Основные составляющие национальных интересов Российской Федерации в информационной сфере. Информационная безопасность Российской Федерации. Интересы личности в информационной сфере. Интересы общества в информационной сфере. Интересы государства в информационной сфере. Виды угроз информационной безопасности Российской Федерации. Источники угроз информационной безопасности Российской Федерации.

Внешние источники угроз. Внутренние источники угроз. Направления обеспечения информационной безопасности государства. Проблемы региональной информационной безопасности.

Тема 3. Основные понятия и общеметодологические принципы теории информационной безопасности. Источники понятий в области информационной безопасности. Основные понятия информационной безопасности: документированная информация, безопасность информации, конфиденциальность, целостность, доступность информации, защита информации, система защиты информации. Общеметодологические принципы теории информационной безопасности.

Тема 4. Понятие и виды защищаемой информации. Понятие и сущность защищаемой информации. Права и обязанности обладателя информации. Виды защищаемой информации: государственная тайна, служебная тайна, профессиональная тайна, коммерческая тайна, персональные данные. Перечень сведений конфиденциального характера. Понятие интеллектуальной собственности и особенности ее защиты.

Модуль 2. Информационная война, методы и средства ее ведения

Раздел 2. Информационная война, методы и средства ее ведения.
АРС: Л - 6 ч., СЗ - 3×2 = 6 ч., СРС: ИТМ - 6 ч., ИЗМ (ИЗМ-2) - 10 ч.

Тема 5. Понятие и виды угроз информационной безопасности. Понятие угрозы информационной безопасности. Фактор, воздействующий на защищаемую информацию. Типы дестабилизирующих факторов. Классификация и виды угроз информационной безопасности. Внутренние и внешние источники угроз информационной безопасности. Угрозы утечки информации и угрозы несанкционированного доступа. Основные элементы канала реализации угрозы безопасности информации.

Тема 6. Информационная безопасность и информационное противоборство. Субъекты информационного противоборства. Цели информационного противоборства. Составные части и методы информационного противоборства. Информационное оружие, его классификация и возможности.

Тема 7. Обеспечение информационной безопасности объектов информационной сферы государства в условиях информационной войны. Методы нарушения конфиденциальности, целостности и доступности информации. Причины, виды, каналы утечки и искажения информации. Основные направления обеспечения информационной безопасности объектов информационной сферы государства в условиях информационной войны. Компьютерная система как объект информационной войны.

Модуль 3. Обеспечения информационной безопасности компьютерных систем

Раздел 3. Обеспечения информационной безопасности компьютерных систем.
АРС: Л - 10 ч., СЗ - 5×2 = 10 ч., ПЗ - 2×2 = 4 ч.,
СРС: ИТМ - 10 ч. ИЗМ (ИЗМ-3) - 10 ч.

Тема 8. Методы и средства обеспечения информационной безопасности компьютерных систем. Компьютерная система как объект информационной безопасности. Общая характеристика способов и средств защиты информации. Правовая, техническая, криптографическая, физическая защита информации. Организационно-правовые, технические и криптографические методы обеспечения информационной безопасности. Программно-аппаратные средства обеспечения информационной безопасности.

Тема 9. Механизмы защиты информации в автоматизированных системах. Содержание сервисов безопасности программно-технического уровня. Идентификация и аутентификация, управление доступом и авторизация, протоколирование и аудит. Криптография для сервисов безопасности: шифрование и контроль целостности. Экранирование. Анализ защищенности. Обеспечение доступности. Туннелирование. Управление.

Тема 10. Формальные модели безопасности автоматизированных систем. Назначение формальных моделей безопасности. Политика безопасности. Монитор безопасности обращений. Дискреционная и мандатная модели безопасности. Формальные модели управления доступом. Модель Харрисона-Руззо-Ульмана. Модель Белла-ЛаПадулы. Формальные модели целостности. Модель Кларка-Вилсона. Модель Биба. Совместное использование моделей безопасностию Ролевое управление доступом.

Тема 11. Методы и критерии оценки защищенности компьютерных систем. Модели, стратегии и системы обеспечения информационной безопасности. Критерии и классы защищенности средств вычислительной техники и автоматизированных информационных систем. Критерии безопасности компьютерных систем «Оранжевая книга». Общие критерии безопасности информационных технологий. Руководящие документы Гостехкомиссии (ФСТЭК) России. Стандарты по управлению информационной безопасностью ISO/IEC 27000.

Тема 12. Защита информации, обрабатываемой в автоматизированных системах от технических разведок. Классификация и возможности технических разведок. Компьютерная разведка. Технические каналы утечки информации при эксплуатации автоматизированных систем. Электромагнитное воздействие и эффекты его воздействия. Защита автоматизированных систем и средств вычислительной техники от внешнего электромагнитного воздействия.

4.3. Перечень тем практических занятий (семинаров)

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

№ п/п	Номер темы дисциплины	Наименование темы практического занятия (семинара)
1	1	Национальная безопасность Российской Федерации
2	2	Основы государственной политики и угрозы безопасности Российской Федерации в информационной сфере
3	3	Основные понятия и общеметодологические принципы теории информационной безопасности
4	4	Понятие и виды защищаемой информации (ПЗ)
5	5	Понятие и виды угроз информационной безопасности (ПЗ)
6	6	Информационная безопасность и информационное противоборство
7	7	Обеспечение информационной безопасности объектов информационной сферы государства в условиях информационной войны
8	8	Методы и средства обеспечения информационной безопасности компьютерных систем
9	9	Механизмы защиты информации в автоматизированных системах (ПЗ)
10	10	Формальные модели безопасности автоматизированных систем
11	10	Особенности дискреционной и мандатной модели безопасности (ПЗ)
12	11	Методы и критерии оценки защищенности компьютерных систем
13	11	Руководящие документы ФСТЭК России (Гостехкомиссии) (ПЗ)
14	12	Защита информации, обрабатываемой в автоматизированных системах от технических разведок

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: Виды безопасности в различных сферах жизнедеятельности личности, общества и государства	2
2	ИТМ: Проблемы региональной информационной безопасности	2
3	ИТМ: Основные понятия информационной безопасности	2
4	ИТМ: Виды защищаемой информации и защита интеллектуальной собственности	2
4	ИЗМ: В соответствии с перечнем тем для модуля 1, п.п. 4.5.1	10
5	ИТМ: Угрозы информационной безопасности Российской Федерации в различных сферах	2
6	ИТМ: Методы информационного противоборства и применение информационного оружия	2
7	ИТМ: Компьютерная система как объект информационной войны	2
7	ИЗМ: В соответствии с перечнем тем для модуля 2, п.п. 4.5.1	10
8	ИТМ: Программно-аппаратные средства обеспечения информационной безопасности	2
9	ИТМ: Механизмы защиты информации компьютерных систем	2
10	ИТМ: Формальные модели обеспечения информационной безопасности	2
11	ИТМ: Стандарты по управлению информационной безопасностью ISO/IEC 27000	2
12	ИТМ: Защита автоматизированных систем и средств вычислительной техники от внешнего электромагнитного воздействия	2
12	ИЗМ: В соответствии с перечнем тем для модуля 3, п.п. 4.5.1	10
	Итого: в **ч** / в **ЗЕ**	**54/1,5**

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

Раздел 1, модуль 1

1. Место и роль информационной безопасности в различных сферах жизнедеятельности личности (общества, государства).
2. Национальная безопасность. Сущность и виды безопасности.
3. Информационная безопасность в системе национальной безопасности РФ.

4. Влияние процессов информатизации общества на составляющие информационной безопасности.
5. Состав и содержание направлений информационной безопасности.
6. Правовая база обеспечения информационной безопасности личности (общества, государства).
7. Государственная информационная политика. История, становление, сущность и содержание, основные направления.
8. Виды информации с точки зрения информационной безопасности.
9. Виды защищаемой информации.
10. Интересы личности (общества, государства) в информационной сфере.
11. Проблемы региональной информационной безопасности.
12. Основные нормативно-правовые акты в области информационной безопасности.
13. Исторические этапы развития системы защиты информации в России.
14. Экономические факторы обеспечения безопасности коммерческой организации.

Раздел 2, модуль 2

1. Угрозы информационной безопасности и факторы, воздействующие на информацию.
2. Причины, виды, каналы утечки и искажение информации.
3. Информационное оружие, его классификация и возможности.
4. Информационное противоборство.
5. Методы нарушения конфиденциальности (целостности, доступности) информации.
6. Национальные интересы РФ и угрозы национальной безопасности.
7. Угрозы информационной безопасности Российской Федерации.
8. Анализ угроз информационной безопасности компьютерных систем.
9. Внешние (внутренние) источники угроз информационной безопасности государства.
10. Актуальные проблемы безопасности компьютерных систем.
11. Актуальные проблемы информационной безопасности при использовании мобильных средств связи.
12. Актуальные проблемы информационной безопасности в социальных сетях.
13. Актуальные проблемы информационной безопасности критически важных объектов.
14. Компьютерная система как объект информационного воздействия.

Раздел 3, модуль 3

1. Основные направления обеспечения информационной безопасности объектов информационной сферы государства в условиях информационной войны.
2. Современные методы и средства защиты информации.
3. Задачи подготовки специалистов по защите информации.
4. Отечественные и зарубежные стандарты в области информационной безопасности.
5. Правовые основы защиты персональных данных.
6. Криптология и основные этапы ее становления и развития.
7. Комплексный подход к обеспечению информационной безопасности.
8. Основные механизмы и сервисы защиты информации.
9. Правовое обеспечение информационной безопасности.
10. Инженерно-техническое обеспечение информационной безопасности.
11. Организация физической защиты информации.
12. Организация работы с персоналом в системе информационной безопасности.
13. Политика информационной безопасности предприятия и организации.
14. Правовые (организационно-технические, экономические) методы обеспечения информационной безопасности.
15. Обеспечение информационной безопасности компьютерных систем.
16. Анализ современных подходов к построению систем защиты информации.
17. Критерии оценки защищенности компьютерных систем, методы и средства обеспечения их информационной безопасности.

18. Особенности обеспечения информационной безопасности компьютерных систем при обработке информации, составляющей государственную тайну.
19. Обеспечение безопасности технических систем и человека в условиях использования информационного оружия.
20. Анализ факторов, определяющих безопасность технических систем.
21. Классификация и возможности технических разведок.
22. Показатели защищенности средств вычислительной техники от НСД к информации.
23. Пароль как средство защиты от НСД.
24. Требования по защите информации в автоматизированных системах от НСД.
25. Оценка безопасности информационных технологий по Общим критериям.

4.5.2 Перечень тем курсовых работ (проектов)

Не предусмотрены.

5 Образовательные технологии, используемые для формирования компетенций

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

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

6 Управление и контроль освоения компетенций

6.1 Текущий контроль освоения заданных дисциплинарных компетенций

Текущий контроль освоения дисциплинарных компетенций проводится в следующих формах:

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

– оценка работы студента на лекционных, практических и семинарских занятиях в рамках рейтинговой системы.

6.2 Рубежный и промежуточный контроль освоения заданных дисциплинарных компетенций

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

– отчет за индивидуальное задание по модулю (модуль 1, 2, 3);

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

6.3 Итоговый контроль освоения заданных дисциплинарных компетенций

1) **Зачёт**

Не предусмотрен.

2) **Экзамен**

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

Экзамен по дисциплине проводится устно по билетам. Билет содержит два теоретических вопроса.

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

Перечень экзаменационных вопросов:

1. Понятие национальной безопасности Российской Федерации.
2. Национальные интересы РФ и стратегические национальные приоритеты.
3. Роль информационной безопасности в обеспечении национальной безопасности государства.
4. Основные составляющие национальных интересов Российской Федерации в информационной сфере.
5. Понятие информационной безопасности Российской Федерации.
6. Интересы личности общества и государства в информационной сфере.
7. Виды угроз информационной безопасности Российской Федерации.
8. Внешние и внутренние источники угроз информационной безопасности Российской Федерации.
9. Методы обеспечения информационной безопасности Российской Федерации
10. Источники понятий в области информационной безопасности.
11. Основные понятия информационной безопасности.
12. Общеметодологические принципы теории информационной безопасности.
13. Понятие и сущность защищаемой информации.
14. Права и обязанности обладателя информации.
15. Виды защищаемой информации.
16. Перечень сведений конфиденциального характера.
17. Понятие интеллектуальной собственности и особенности ее защиты.
18. Понятие угрозы информационной безопасности.
19. Фактор, воздействующий на защищаемую информацию. Типы дестабилизирующих факторов.
20. Классификация и виды угроз информационной безопасности.
21. Внутренние и внешние источники угроз информационной безопасности.
22. Угрозы утечки информации и угрозы несанкционированного доступа.
23. Основные элементы канала реализации угрозы безопасности информации.
24. Субъекты и цели информационного противоборства.
25. Составные части и методы информационного противоборства.
26. Информационное оружие, его классификация и возможности.
27. Методы нарушения конфиденциальности, целостности и доступности информации.
28. Информационная война как способ воздействия на информационные системы.
29. Информационная безопасность критически важных объектов.
30. Обеспечение безопасности объектов информационной сферы государства в информационной войне.
31. Компьютерная система как объект информационной безопасности.
32. Основные способы защиты информации.
33. Понятие и классификация средств защиты информации.

34. Характеристика средств защиты информации.
35. Уровни информационной безопасности и их характеристика.
36. Сервисы безопасности программно-технического уровня.
37. Идентификация и аутентификация как сервисы безопасности.
38. Управление доступом и его виды.
39. Авторизация как сервис безопасности.
40. Протоколирование и аудит как сервисы безопасности.
41. Криптографические сервисы безопасности.
42. Экранирование как сервис безопасности.
43. Анализ защищенности как сервис безопасности.
44. Туннелирование как сервис безопасности.
45. Управление как сервис безопасности.
46. Назначение формальных моделей безопасности. Политика безопасности.
47. Дискреционная модель безопасности. Модель Харрисона-Руззо-Ульмана.
48. Мандатная модель безопасности. Модель Белла-ЛаПадулы.
49. Формальные модели целостности.
50. Понятие ролевого управления доступом.
51. Модели, стратегии и системы обеспечения информационной безопасности.
52. Критерии безопасности компьютерных систем «Оранжевая книга».
53. Общие критерии безопасности информационных технологий.
54. Критерии и классы защищенности СВТ и АС. Руководящие документы ФСТЭК России.
55. Стандарты по управлению информационной безопасностью ISO/IEC 27000.
56. Классификация и возможности технических разведок.
57. Компьютерная разведка.
58. Технические каналы утечки информации при эксплуатации автоматизированных систем.
59. Электромагнитное воздействие и эффекты его воздействия.
60. Защита автоматизированных систем и средств вычислительной техники от внешнего электромагнитного воздействия.

Пример экзаменационного билета:

ПЕРМСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ

Электротехнический факультет

Кафедра автоматики и телемеханики

Экзамен по дисциплине «Основы информационной безопасности»

Экзаменационный билет № 1

1. Понятие национальной безопасности Российской Федерации.
2. Компьютерная система как объект информационной безопасности.

Заведующий кафедрой
д-р техн. наук, профессор А.А. Южаков

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

Таблица 6.1 - Виды контроля освоения элементов и частей компетенций

Контролируемые результаты освоения дисциплины (ЗУВы)	Вид контроля					
	ТО	РТ	КР	ПЗ	От	Экз
1	2	3	4	5	6	7
В результате освоения дисциплины студент						
Знает:						
– роль специалиста по защите информации, цели и смысл государственной службы, место информационной безопасности в системе национальной безопасности страны;	+	+				+
– угрозы информационной безопасности государства;	+	+				+
– содержание информационной войны, методы и средства ее ведения;	+	+				+
– виды информации ограниченного доступа, основные понятия в области информационной безопасности и методологические принципы создания систем защиты информации;	+	+				+
– методы, средства защиты информации, критерии оценки защищенности компьютерных систем;	+	+				+
Умеет:						
– анализировать информацию по вопросам национальной и информационной безопасности государства;			+	+		+
– анализировать угрозы безопасности информационной инфраструктуры государства;			+	+		+
– выбирать критерии оценки защищенности информационной инфраструктуры государства;			+	+		+
– выбирать и анализировать показатели качества и критерии оценки систем и отдельных методов и средств защиты информации;			+	+		+
– пользоваться современной научно-технической литературой для решения задач защиты информации;			+	+		+
Владеет:						
– навыками активной состязательной деятельности в условиях информационного противоборства;				+	+	+
– навыками подбора нормативных и методических материалов по вопросам обеспечения информационной безопасности.				+	+	+

ТО – текущий опрос (контроль знаний по теме);

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

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

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

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

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		**24**
Вып. инд. заданий (ИЗМ)	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2				**30**
КСР																2			**2**
Модуль:	**1**					**2**				**3**									
Контр. тестирование					+					+							+		
Дисциплин. контроль																			**Экз.**

8. Учебно-методическое и информационное обеспечение дисциплины

8.1. Карта обеспеченности дисциплины учебно-методической литературой

Основы информационной безопасности	*Профессиональный цикл*	
полное название дисциплины	[x] обязат [ ] по выбору студента	[x] базовая часть цикла [ ] вариативная часть цикла

090900.62 090303.65	«Информационная безопасность» «Информационная безопасность автоматизированных систем»
код направления / специальности	*полное название направления/ специальности*

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

2013 семестр (ы) 4 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	Галатенко В.А. Основы информационной безопасности М: ИНТУИТ: БИНОМ. Лаб. знаний, 2012.- 205 с.	2
1	Галатенко В.А. Основы информационной безопасности М: ИНТУИТ: БИНОМ. Лаб. знаний, 2006.- 205 с.	4
2	Белов Е.Б. и др. Основы информационной безопасности М. : Горячая линия-Телеком, 2006 .— 544 с.	25
3	Данилов А.Н., Данилова С.А., Зорин А.А. Основы информационной безопасности. Пермь: ПГТУ, 2008.-555 с.	99
2. Дополнительная литература		
	2.1. Учебные и научные издания	
1	Герасименко В. А. и др. Основы защиты информации М.: Изд-во МИФИ, 1997 — 537 с.	2
2	Цирлов В.Л. Основы информационной безопасности: краткий курс. Ростов-на-Дону : Феникс, 2008 .— 254 с.	8
3	Расторгуев С.П. Информационная война М. : Радио и связь, 1999 .— 415 с.	1
4	Данилов А.Н., Полшков А.В., Шабуров А.С. Информационная безопасность Пермь: ПГТУ, 2004.-150 с.	4
5	Ярочкин В. И. Информационная безопасность: учебник для вузов, 5-е изд. - М: Акад. проект, 2008. - 543 с.	21
	2.2. Периодические издания	
1	Интеллектуальная собственность (Авторское право)	
2	Интеллектуальная собственность (Промышленная собственность)	
	2.3. Нормативно-технические издания	
	2.4. Официальные издания	
1	Стратегия национальной безопасности Российской Федерации до 2020 года	
2	Доктрина информационной безопасности Российской Федерации	

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

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

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	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
1.		
2.		
3.		
4.		
5.		

Лист регистрации изменений

№ п.п	Содержание изменения	Дата, номер протокола заседания кафедры. Подпись заведующего кафедрой
1.	Содержание стр. 1, кроме абзацев 6-9, изложить в редакции, приведенной на стр. 1а.	Протокол заседания кафедры АТ от «16 » января 2017 г. № 18 Зав. кафедрой АТ д-р техн. наук, проф. _____ А.А. Южаков
	Содержание стр. 2 (абзацы 1-5) изложить в редакции, приведенной на стр. 2а.	
	Изменения шифров и формулировок компетенций (стр. 3- 5, 7-9,) внесены на основании перехода на ФГОС ВО: **по направлению подготовки 10.03.01, утвержденный приказом Министерства образования и науки РФ от 01.12.2016 г. № 1515, и обновления базового учебного плана подготовки бакалавров по направлению 10.03.01, утвержденного 22.16.2016 г.:** - общекультурную компетенцию ОК-7 считать общекультурной компетенцией ОК-5 с формулировкой: «Способность понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики»; - изменить шифр дисциплинарной компетенции с ОК-7.Б3.В2 на ОК-5.Б1.Б.21; - профессиональную компетенцию ПК-24 считать профессиональной компетенцией ПК-9 с формулировкой «Способность осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности»; - изменить шифр дисциплинарной компетенции с ПК-24.Б3.В2 на ПК-9.Б1.Б.21; **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.:** - общекультурную компетенцию ОК-5 считать общекультурной компетенцией ОК-5 с формулировкой «Способность понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики»; - изменить шифр дисциплинарной компетенции с ОК-5.С3.В2 на ОК-5.Б1.Б23;	

- профессиональную компетенцию ПК-9 считать профессиональной компетенции ПК-1 с формулировкой «Способность осуществлять поиск, изучение, обобщение и систематизацию научно-технической информации, нормативных и методических материалов в сфере профессиональной деятельности, в том числе на иностранном языке»; - изменить шифр дисциплинарной компетенции с ПК-9.С3.В2 на ПК-1.Б1.Б23.
Наименование раздела 1.4 «Место учебной дисциплины в структуре профессиональной подготовки выпускников» изложить в следующей редакции: «Место учебной дисциплины в структуре образовательной программы».
В первом абзаце раздела 1.4 заменить слова «цикла профессиональных дисциплин» на «блока 1. Дисциплины (модули)». Шифр названия направления и специальности читать в новой редакции.
Наименование раздела 2 «Требования к результатам освоения учебной дисциплины» изложить в следующей редакции: «Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы».
Раздел 3 «Структура учебной дисциплины по видам и формам учебной работы» дополнить новым абзацем следующего содержания: «Объем дисциплины в зачетных единицах составляет 4 ЗЕ. Количество часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся указано в таблице 3.1.».
В табл. 3.1.: а) строку п. 1 дополнить словами «(контактная работа)»; б) строку п. 3 изложить в следующей редакции: «Итоговый контроль (промежуточная аттестация обучающихся) по дисциплине:».
В табл. 4.1.: а) в строке п. 1 «Количество часов (очная форма обучения)» дополнить словами «и виды занятий»; б) «Итоговая аттестация» заменить на «Итоговый контроль (промежуточная аттестация).
В раздел 4.5 «Распределение тем по видам самостоятельной работы» добавить параграф с наименованием «Методические указания для обучающихся по изучению дисциплины» следующего содержания: «При изучении дисциплины обучающимся целесообразно выполнять следующие рекомендации: 1. Изучение учебной дисциплины должно вестись систематически. 2. После изучения какого-либо раздела по учебнику или конспектным материалам рекомендуется по памяти воспроизвести основные термины, определения, понятия раздела. 3. Особое внимание следует уделить выполнению отчетов по практическим занятиям, лабораторным работам и индивиду-

	альным комплексным заданиям на самостоятельную работу. 4. Изучение дисциплины осуществляется в течение одного семестра, график изучения дисциплины приводится п. 7. 5. Вся тематика вопросов, изучаемых самостоятельно, задается на лекциях преподавателем. Им же даются источники (в первую очередь вновь изданные в периодической научной литературе) для более детального понимания вопросов, озвученных на лекции.»	
	Наименование раздела 6 изложить в следующей редакции: «Фонд оценочных средств дисциплины».	
	Наименование параграфа 6.1 изложить в редакции «Текущий и рубежный контроль освоения заданных дисциплинарных частей компетенций».	
	В параграф 6.1 добавить первый абзац следующего содержания: «Текущий контроль осуществляется путем устного опроса во время аудиторных занятий».	
	Наименование раздела 8 Учебно-методическое и информационное обеспечение дисциплины» изложить в следующей редакции: «Перечень учебно-методического и информационного обеспечения для самостоятельной работы обучающихся по дисциплине».	
	Изменить название раздела «Список изданий» на «8.2. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины».	
	Добавить в таблицу 8.1 строку «2.5 Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины».	
	Дополнить п. 2.5 таблицы строками: **Электронная библиотека** Научной библиотеки Пермского национального исследовательского политехнического университета [Электронный ресурс: полнотекстовая база данных электрон. документов, изданных в Изд-ве ПНИПУ]. – Электрон. дан. (1 912 записей). – Пермь, 2014. – Режим доступа: http://elib.pstu.ru/. – Загл. с экрана. **Лань** [Электронный ресурс: электрон. -библ. система: полнотекстовая база данных электрон. документов по гуманит., естеств., и техн. наукам] / Изд-во «Лань». – Санкт-Петербург: Лань, 2010- . – Режим доступа: http://e.lanbook.com/. – Загл. с экрана. **Консультант Плюс** [Электронный ресурс : справочная правовая система : документы и комментарии : универсал. информ. ресурс]. – Версия Проф, сетевая. – Москва, 1992. – Режим доступа: Компьютер. сеть Науч. б-ки Перм. нац. исслед. политехн. ун-та, свободный.».	
	Раздел 8.2 «Компьютерные обучающие и контролирующие программы» считать разделом 8.3 и наименование изложить в следующей редакции: «Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине».	

	Раздел 8.3 «Программные инструментальные средства» считать разделом 8.4 «Перечень программного обеспечения, в том числе компьютерные обучающие и контролирующие программы».	
	Раздел 8.4 «Аудио- и видео-пособия» считать разделом 8.5.	
	Наименование раздела 9 изложить в следующей редакции: «Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине».	
2.		
3.		
4.		
5.		
6.		
7.		
8.		