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
«16» 09 2015 г.

УЧЕБНО-МЕТОДИЧЕСКИЙ КОМПЛЕКС ДИСЦИПЛИНЫ
«Внутренний аудит систем защиты информации на соответствие стандартам»

Основная образовательная программа подготовки специалистов
Специальность: 090303.65 «Информационная безопасность автоматизированных систем»

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

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

Курс: 4 Семестр: 8

Трудоёмкость:
Кредитов по рабочему учебному плану: 5 ЗЕ
Часов по рабочему учебному плану: 180 ч

Виды контроля:
Экзамен: 8 семестр Зачёт: - Курсовой проект: - Курсовая работа: -

**Пермь
2015**

Рабочая программа дисциплины «Внутренний аудит систем защиты информации на соответствие стандартам» разработана на основании:

- федерального государственного образовательного стандарта высшего профессионального образования утвержденного приказом Министерства образования и науки Российской Федерации «17» января 2011г. № 60, по направлению подготовки (специальности) 090303 «Информационная безопасность автоматизированных систем» (квалификация (степень) «специалист»);
- компетентностной модели выпускника ООП по специальности 090303.65 - «Информационная безопасность автоматизированных систем», специализации «Обеспечение информационной безопасности распределенных информационных систем», утвержденной «24» июня 2013 г.;
- рабочего учебного плана очной формы обучения по специальности 090303.65 - «Информационная безопасность автоматизированных систем», специализации «Обеспечение информационной безопасности распределенных информационных систем», утвержденного «29» августа 2011 г.

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

Разработчик канд. техн. наук _____ Зорин А.А.

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 «08» 09 2015 г., протокол № 41
Председатель методической комиссии
электротехнического факультета,
канд. техн. наук, профессор _____ Гольдштейн А.Л.

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

1 Общие положения

1.1 Цель дисциплины – освоение дисциплинарных компетенций по применению комплекса мероприятий внутреннего аудита систем защиты информации на соответствие стандартам.

В процессе изучения данной дисциплины студент осваивает следующие компетенции:

- способность применять методологию научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами (ПК-5);
- способность проводить анализ защищенности автоматизированных систем (ПК-12);
- способность проводить синтез и анализ проектных решений по обеспечению безопасности автоматизированных систем (ПК-17).

1.2 Задачи дисциплины:

- изучение основных положений, понятий и категорий теоретических основ функционирования систем информационной безопасности в организациях;
- изучение основ и принципов организации современных проблем организационного обеспечения информационной безопасности;
- изучение организации работы и порядка применения терминологии организационного обеспечения информационной безопасности;
- изучение целей систем организационной защиты информации в организациях;
- изучение основных направлений и методов организационной защиты информации в организациях, формирование умений в разработке проектов функционирования систем организационной защиты информации в организациях;
- формирование навыков работы в организации процессов управления системами организационной защиты информации в организациях.

1.3 Предметом освоения дисциплины являются следующие объекты:

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

1.4 Место дисциплины в структуре профессиональной подготовки выпускников.

Дисциплина «Внутренний аудит систем защиты информации на соответствие стандартам» относится к циклу профессиональных дисциплин и является дисциплиной по выбору студента при освоении ООП по специальности 090303.65 – Информационная безопасность автоматизированных систем. После изучения дисциплины обучающийся должен освоить части указанных в пункте 1.1 компетенций и демонстрировать следующие результаты:

знать:

– основные факторы, определяющие величину ущерба, нанесенного организациям вследствие отсутствия или недостаточной надёжности систем защиты информации;

– основы анализа состояния безопасности в организациях;

– теоретические основы функционирования систем информационной безопасности в организациях, ее современные проблемы и терминология;

– основы законодательства Российской Федерации по защите информации;

– цели, функции и процессы управления системами информационной безопасности в организациях;

– основные направления и методы информационной безопасности в организациях;

***уметь*:**

– анализировать эффективность систем информационной безопасности в организациях;

– разрабатывать нормативно-методические материалы по регламентации системы информационной безопасности в организациях;

– организовывать работу с персоналом, обладающим конфиденциальной информацией;

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

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

– организовывать охрану персонала, территорий, зданий, помещений организаций;

– организовывать и проводить служебное расследование по фактам разглашения, утечки информации и несанкционированного доступа к ней;

– организовывать и проводить аналитическую работу по предупреждению утечки конфиденциальной информации;

иметь навыки:

– выбора метода определения ущерба, наносимого владельцу информации в результате противоправного ее использования;

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

– организации доступа к объектам информатизации и обеспечения режима секретности, организации и управления деятельностью службы защиты информации в организациях.

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

Таблица 1.1 – Дисциплины, направленные на формирование компетенций

Код компетенции	**Наименование компетенции**	**Предшествующие дисциплины**	**Последующие дисциплины (группы дисциплин)**
Профессиональные компетенции			
ПК-5.	способен применять методологию научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными про-	НИРС	Междисциплинарный государственный экзамен
ПК-12	способен проводить анализ защищенности автоматизированных систем	НИРС	Междисциплинарный государственный экзамен

ПК-17.	способен проводить синтез и анализ проектных решений по обеспечению безопасности автоматизированных систем	Программирование и основы алгоритмизации (методы и технологии программи-	Программно-аппаратные средства защиты информации

2 Требования к результатам освоения учебной дисциплины

Учебная дисциплина обеспечивает формирование заданных частей общекультурных и профессиональных компетенций (ПК-5.С3.ДВ.01.2, ПК-12.С3.ДВ.01.2 и ПК-17.С3.ДВ.01.2).

2.1 Карты дисциплинарных компетенций

2.1.1 Карта дисциплинарной компетенции ПК-5.С3.ДВ.01.2

Код	Формулировка компетенции:
ПК-5.	способен применять методологию научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами.

Код	Формулировка дисциплинарной части компетенции:
ПК-5-2.С3.ДВ.01.2	способен применять методологию научных исследований к обобщению, анализу, критическому осмыслению информации, систематизации, прогнозированию, постановке аналитических задач и выбору путей их решения, в том числе в работе над междисциплинарными и инновационными проектами

2.1.2 Компонентный состав дисциплинарной компетенции

Перечень компонентов	Виды учебной работы	Средства контроля
Знать: – основные факторы, определяющие величину ущерба, нанесенного организациям вследствие отсутствия или недостаточной надёжности систем защиты информации (ПК-5-2-1з.С3.ДВ.01.2); – основы анализа состояния безопасности в организациях (ПК-5-2-2з.С3.ДВ.01.2).	Лекции; семинарские и практические занятия; самостоятельное изучение теоретического материала.	Экзамен; отчет по выполнению практических задач, обсуждение результатов самостоятельного изучения теоретического материала в ходе ПЗ и СЗ. Вопросы для текущего, рубежного и итогового контроля
Уметь: – анализировать эффективность систем информационной безопасности в организациях (ПК-5-2-1у.С3.ДВ.01.2); – разрабатывать нормативно-методические материалы по регламентации системы информационной безопасности в организациях (ПК-5-2-2у.С3.ДВ.01.2); – организовывать работу с персоналом, обладающим конфиденциальной информацией (ПК-5-2-3у.С3.ДВ.01.2).	Практические занятия; Самостоятельная работа студентов по решению практических задач. Самостоятельная работа студентов по выполнению индивидуальных заданий по модулю. Самостоятельная работа студентов	Защита отчета по выполнению индивидуального задания и отчета по практическому заданию. Вопросы итогового контроля

	по подготовке к экзамену	
Владеть: – навыками выбора метода определения ущерба, наносимого владельцу информации в результате противоправного ее использования (ОК-10-2-1в.С3.ДВ.01.2).	Выполнение индивидуального комплексного задания.	Защита отчета по индивидуальному комплексному заданию.

2.2.1 Карта дисциплинарной компетенции ПК-12.С3.ДВ.01.2

Код	Формулировка компетенции:
ПК-12.[illegible]	способен проводить анализ защищенности автоматизированных систем

Код	Формулировка дисциплинарной части компетенции
ПК-12-1.С3.ДВ.01.2	способен использовать требованиям государственных или корпоративных нормативных документов для анализа защищенности автоматизированных систем

2.2.2 Компонентный состав дисциплинарной компетенции

Перечень компонентов	Виды учебной работы	Средства оценки
Знать: – теоретические основы функционирования систем информационной безопасности в организациях, ее современные проблемы и терминология (ПК-12-1-1з.С3.ДВ.01.2); – основы законодательства Российской Федерации по защите информации (ПК-12-1-2з.С3.ДВ.01.2).	Лекции; семинарские и практические занятия; самостоятельное изучение теоретического материала.	Экзамен; отчет по выполнению практических задач, обсуждение результатов самостоятельного изучения теоретического материала в ходе ПЗ и СЗ. Вопросы для текущего, рубежного и итогового контроля
Уметь: – разрабатывать проекты нормативных и организационно-распорядительных документов, регламентирующих работу по защите информации в организациях (ПК-12-1-1у.С3.ДВ.01.2); – применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности организаций (ПК-12-1-2у.С3.ДВ.01.2).	Практические занятия; Самостоятельная работа студентов по решению практических задач. Самостоятельная работа студентов по выполнению индивидуальных заданий по модулю. Самостоятельная работа студентов по подготовке к экзамену	Защита отчета по выполнению индивидуального задания и отчета по практическому заданию. Вопросы итогового контроля

Владеть: – навыками работы с персоналом, принятия организационно-управленческих решений, в том числе в нестандартных ситуациях в целях обеспечения информационной безопасности в организациях (ПК-12-1-1в.С3.ДВ.01.2).	Выполнение индивидуального комплексного задания.	Защита отчета по индивидуальному комплексному заданию.

2.3.1 Карта дисциплинарной компетенции ПК-17.С3.ДВ.01.2

Код	Формулировка компетенции:
ПК-17.(	способен проводить синтез и анализ проектных решений по обеспечению безопасности автоматизированных систем

Код	Формулировка дисциплинарной части компетенции
ПК-17-1.С3.ДВ.01.2	способен проводить синтез и анализ проектных решений по обеспечению безопасности автоматизированных систем в организациях

2.3.2 Компонентный состав дисциплинарной компетенции

Перечень компонентов	Виды учебной работы	Средства оценки
Знать: – цели, функции и процессы управления системами информационной безопасности в организациях (ПК-17-1-1з.С3.ДВ.01.2); – основные направления и методы информационной безопасности в организациях (ПК-17-1-2з.С3.ДВ.01.2).	Лекции; семинарские и практические занятия; самостоятельное изучение теоретического материала.	Экзамен; отчет по выполнению практических задач, обсуждение результатов самостоятельного изучения теоретического материала в ходе ПЗ и СЗ. Вопросы для текущего, рубежного и итогового контроля
Уметь: – организовывать охрану персонала, территорий, зданий, помещений организаций (ПК-17-1-1у.С3.ДВ.01.2); – организовывать и проводить служебное расследование по фактам разглашения, утечки информации и несанкционированного доступа к ней (ПК-17-1-2у.С3.ДВ.01.2); – организовывать и проводить аналитическую работу по предупреждению утечки конфиденциальной информации (ПК-17-1-3у.С3.ДВ.01.2).	Практические занятия; Самостоятельная работа студентов по решению практических задач. Самостоятельная работа студентов по выполнению индивидуальных заданий по модулю. Самостоятельная работа студентов по подготовке к экзамену	Защита отчета по выполнению индивидуального задания и отчета по практическому заданию. Вопросы итогового контроля

Владеть: – организацией доступа к объектам информатизации и обеспечения режима секретности, организации и управления деятельностью службы защиты информации в организациях (ПК-17-1-1в.С3.ДВ.01.2).	Выполнение индивидуального комплексного задания.	Защита отчета по индивидуальному комплексному заданию.

3 Структура учебной дисциплины по видам и формам 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 – Структура дисциплины по объёмам и видам учебной работы

№ п.п.	Виды учебной работы	Трудоёмкость, ч	Форма представления результатов
1	2	3	4
1	**Аудиторная работа**	**72**	
	- в том числе в интерактивной форме	36	
	- лекции (Л)	32	конспект лекций
	- в том числе в интерактивной форме	16	
	- практические занятия (ПЗ), семинарские занятия (СЗ)	36	отчёт о выполнении
	- в том числе в интерактивной форме	16	
	Контроль самостоятельной работы (КСР)	4	
2	**Самостоятельная работа студентов** (СРС)	**72**	
	- самостоятельное изучение теоретического материала (ИТМ)	36	отчет по вопросам для текущего и рубежного контроля
	- выполнение индивидуальных заданий по модулю (ИЗМ)	36	отчёт о выполнении
3	Итоговая аттестация по дисциплине	**36**	**Экзамен**
4	**Трудоёмкость дисциплины, всего:** **в часах (ч)** **в зачётных единицах (ЗЕ)**	**180** **5**	

4 Содержание учебной дисциплины

4.1 Модульный тематический план

Таблица 4.1 – Тематический план по модулям учебной дисциплины

Номер учебного модуля	Номер раздела дисциплины	Номер темы дисциплины	Количество часов (очная форма обучения)							Iотог. 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	Введение		2	2							2
	1	1.1	20	10	10	1	20	10	10		41
	Всего по модулю:		**23**	12	10	1	**20**	10	10		**43**
2	2	2.1	8	4	4		12	6	6		20
		2.2	11	4	6		12	6	6		23
	Всего по модулю:		**19**	8	10	1	**24**	12	12		**43**
3	3	3.1	4	2	2		4	2	2		8
		3.2	8	4	4		8	4	4		16
		3.3	6	2	4		4	2	2		10
		3.4	12	4	6	2	12	6	6		24
	Всего по модулю:		**30**	12	16	2	**28**	14	14		**58**
Итоговая аттестация											**36**
Итого			**72**	**32**	**36**	**4**	**72**	**36**	**36**	**36**	**180/5**

ИЗМ – индивидуальное задание по модулю.
ИТМ – самостоятельное изучение теоретического материала

4.2. Содержание разделов и тем учебной дисциплины

Введение. Л – 2 ч.

Основные понятия, термины и определения. Предмет и задачи дисциплины. Цели и задачи курса и его место в подготовке специалистов по защите информации.

Особенности формирования терминологии научной дисциплины. Взаимосвязь курса с правовыми, историческими, экономическими, социальными, социально-психологическими и техническими дисциплинами учебного плана.

Методические материалы. Периодические издания. Обязательная и дополнительная литература.

Модуль 1. Общие понятия об информационных технологиях.

Раздел I. Общие понятия об информационных технологиях.

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

Тема 1.1 Основные понятия, применяемые в информационных технологиях.

Аппаратное и программное обеспечение вычислительной техники, информационные процессы и информационные технологии. Системное и прикладное программное обеспечение, понятие информационных ресурсов (объектов) и пользователей данных ресурсов (субъектов). Основные функции операционной системы ПЭВМ, встроенные возможности разграничения

доступа, блокировка доступа к рабочей станции. Идентификация и аутентификация пользователей автоматизированных систем, понятие учетных записей, полномочия администраторов и пользователей систем (привилегии, роли), автоматическая блокировка/разблокировка учетных записей. Использование паролей, понятие структуры пароля, правила выбора стойких паролей, подбор паролей с использование специализированных программ. Использование локально-вычислительных сетей, понятие сетевых ресурсов, изолированность сегментов локально-вычислительных сетей, разграничение прав доступа к сетевым ресурсам (на примере сети *Windows*), анализ системных журналов, резервирование и архивирование данных.

Модуль 2. Обеспечение информационной безопасности и защита автоматизированных систем.

Раздел II. Обеспечение информационной безопасности и защита автоматизированных систем.

АРС: Л – 8 ч.; ПЗ (СЗ) – 10 ч., КСР – 1 ч.; СРС: ИТМ – 12 ч., ИЗМ (ИЗМ-2) – 12 ч.

Тема 2.1 Средства криптографической защиты информации.

Шифрование данных при хранении и передачи (симметричное/асимметричное шифрование). Понятие электронно-цифровой подписи, цифровых сертификатов, описание механизмов аутентификации.

Средства криптографической защиты информации в банковской системе.

Тема 2.2 Основные понятия информационной безопасности.

Политика безопасности в системе, критичные информационные ресурсы. Разграничение доступа к ресурсам, понятие несанкционированного доступа и несанкционированного воздействия. Понятие целостности и лицензионной чистоты программного обеспечения.

Модуль 3. Информационная безопасность в организациях.

Раздел III. Информационная безопасность в организациях.

АРС: Л – 12 ч.; ПЗ (СЗ) – 16 ч., КСР – 2 ч.; СРС: ИТМ – 14 ч., ИЗМ (ИЗМ-3) – 14 ч.

Тема 3.1 Теоретические и методологические аспекты основных методов информационной безопасности.

Защита находящейся в системе информации от дестабилизирующего воздействия внешних и внутренних угроз информации. Защита элементов системы от дестабилизирующего воздействия внешних и внутренних информационных угроз. Защита внешней среды от информационных угроз со стороны рассматриваемой системы. Правовое регулирование экономической деятельностью.

Тема 3.2 Автоматизированные системы защиты информации.

Особенности автоматизированных систем защиты информации, используемых в РФ. Информационное обеспечение автоматизированных систем защиты информации. Техническое оснащение современных автоматизированных систем защиты информации. Программное обеспечение автоматизированных систем защиты информации.

Тема 3.3 Достоверность данных технологического процесса эксплуатации ЭИС.

Визуальные и программные методы контроля. Технологический контроль обеспечения информационной безопасности в организациях. Требования к проведению политики безопасности в организациях. Ведение учета использования компьютерных систем. Доверие к компьютерным системам.

Тема 3.4 Реализация требований информационной безопасности в организациях.

Основные направления политики информационной безопасности и нормативная база. Механизмы и методы информационной безопасности, функции администраторов информационной безопасности подразделений. Особенности использования средств защиты информации

от несанкционированного доступа. Организация бесперебойного функционирования информационных систем.

4.3 Перечень тем практических и семинарских занятий

Таблица 4.3 – Темы практических и семинарских занятий

№ п.п.	Номер темы дисциплины	Наименование темы практического (семинарского) занятия
1	2	3
1	1.1	Управление пользователями и группами в ОС Windows 2000/XP/2003/Vista/7/8/10.
2	2.1	Система разграничения доступа к локальным и сетевым ресурсам в ОС Windows 2000/XP/2003/Vista/7/8/10.
3	2.2	Сетевые атаки.
4	3.2	Средства защиты информации от несанкционированного доступа (на примере СЗИ от НСД «Аккорд»).
5	3.4	Работа «Аккорд» с моделированием случаев НСД, нарушением целостности и запуском несанкционированного ПО.

4.4 Перечень тем лабораторных работ

Не предусмотрены.

4.5 Виды самостоятельной работы студентов

Таблица 4.4 – Виды самостоятельной работы студентов (СРС)

Номер темы (раздела) дисциплины	Вид самостоятельной работы студентов	Трудоёмкость, часов
1	2	3
1.1	ИТМ: Перспективы развития законодательства в области информационной безопасности	10
1.1	ИЗМ: В соответствии с перечнем тем для модуля 1, п.п. 4.5.1	10
2.1	ИТМ: Шифрование данных при хранении и передачи (симметричное/асимметричное шифрование).	6
2.1	ИЗМ: В соответствии с перечнем тем для модуля 2, п.п. 4.5.1	6
2.2	ИТМ: Разграничение доступа к ресурсам, понятие несанкционированного доступа и несанкционированного воздействия.	6
2.2	ИЗМ: В соответствии с перечнем тем для модуля 2, п.п. 4.5.1	6
3.1	ИТМ: Правовое регулирование по защите информации в организациях.	2
3.1	ИЗМ: В соответствии с перечнем тем для модуля 3, п.п. 4.5.1	2
3.2	ИТМ: Информационное и техническое обеспечение автоматизированных банковских систем.	4
3.2	ИЗМ: В соответствии с перечнем тем для модуля 3, п.п. 4.5.1	4
3.3	ИТМ: Ведение учета использования компьютерных систем.	2
3.3	ИЗМ: В соответствии с перечнем тем для модуля 3, п.п. 4.5.1	2
3.4	ИТМ: Организация бесперебойного функционирования информационных систем.	6
3.4	ИЗМ: В соответствии с перечнем тем для модуля 3, п.п. 4.5.1	6
	Итого:	**72/2**

	в ч / в ЗЕ	

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

Раздел 1, модуль 1.

1. Понятие операционной системы ПЭВМ
2. Встроенные возможности операционной системы, блокировка доступа к рабочей станции.
3. Идентификация и аутентификация пользователей автоматизированных систем
4. Учетные записи, полномочия администраторов и пользователей систем (привилегии, роли)
5. Специализированных программы по подбору паролей, правила выбора стойких паролей.
6. Разграничение прав доступа к сетевым ресурсам.
7. Анализ системных журналов.
8. Резервирование и архивирование данных.

Раздел 2, модуль 2.

9. Симметричное шифрование данных при хранении и передаче информации.
10. Асимметричное шифрование данных при хранении и передаче информации.
11. Электронно-цифровая подпись.
12. Цифровые сертификаты.
13. Описание механизмов аутентификации.
14. Средства криптографической защиты информации.
15. Политика безопасности.
16. Разграничение доступа к ресурсам, понятие несанкционированного доступа и несанкционированного воздействия.
17. Методы проверки кандидатов на должности, связанные с работой с конфиденциальной информацией.
18. Организация контроля выполнения распорядка дня лицами, работающими в организациях.
19. Каналы разглашения персоналом организаций конфиденциальной информации.

Раздел 3, модуль 3.

20. Правовое регулирование защиты информации.
21. Особенности автоматизированных систем защиты информации, используемых в организации.
22. Информационное обеспечение автоматизированных систем защиты информации.
23. Техническое оснащение современных автоматизированных систем защиты информации.
24. Программное обеспечение автоматизированных систем защиты информации.
25. Основные направления политики информационной безопасности и нормативная база.
26. Стандарты информационной безопасности с учетом изменений в законодательстве.
27. Применяемые меры и средства защиты информации, функции администраторов информационной безопасности подразделений.
28. Особенности использования средств защиты информации от несанкционированного доступа.
29. Организация бесперебойного функционирования информационных систем.

4.6 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. Проведение практических занятий основывается на активном применении обучаемыми студентами руководящих документов Банка 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 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) **Экзамен**

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

Экзамен по дисциплине проводится в виде ответа на вопросы билета. Билет содержит два теоретических вопроса.

Фонды оценочных средств, включающий задания практических занятий, тестовые задания для рубежного контроля и методы оценки, критерии оценивания, перечень контрольных точек и таблица планирования результатов обучения, вопросы к экзамену, позволяющие оценить результаты освоения данной дисциплины, входит в состав УМКД на правах отдельного документа.

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

Таблица 6.1 - Виды контроля освоения элементов и частей компетенций

Контролируемые результаты освоения дисциплины (ЗУВы)	Вид/форма контроля				
	ТО	РТ	ОПЗ	ОИЗМ	Экз.
В результате освоения дисциплины студент					
Знает:					
– основные факторы, определяющие величину ущерба, нанесенного организациям вследствие отсутствия или недостаточной надёжности систем защиты информации (ПК-5-2-1з.С3.ДВ.01.2);	+	+	+		+
– основы анализа состояния безопасности в организациях (ПК-5-2-2з.С3.ДВ.01.2);	+	+	+		+
– теоретические основы функционирования систем информационной безопасности в организациях, ее современные проблемы и терминология (ПК-12-1-1з.С3.ДВ.01.2);	+	+	+		+
– основы законодательства Российской Федерации по защите информации (ПК-12-1-2з.С3.ДВ.01.2);	+	+	+		+
– цели, функции и процессы управления системами информационной безопасности в организациях (ПК-17-1-1з.С3.ДВ.01.2);	+	+	+		+
– основные направления и методы информационной безопасности в организациях (ПК-17-1-2з.С3.ДВ.01.2).	+	+	+		+
Умеет:					
– анализировать эффективность систем информационной безопасности в организациях (ПК-5-2-1у.С3.ДВ.01.2);			+	+	
– разрабатывать нормативно-методические материалы по регламентации системы информационной безопасности в организациях (ПК-5-2-2у.С3.ДВ.01.2);			+	+	
– организовывать работу с персоналом, обладающим конфиденциальной информацией (ПК-5-2-3у.С3.ДВ.01.2);			+	+	
– разрабатывать проекты нормативных и организационно-распорядительных документов, регламентирующих работу по защите информации в организациях (ПК-12-1-1у.С3.ДВ.01.2);			+	+	
– применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности организаций (ПК-12-1-2у.С3.ДВ.01.2);			+	+	
– организовывать охрану персонала, территорий, зданий, помещений организаций (ПК-17-1-1у.С3.ДВ.01.2);			+	+	
– организовывать и проводить служебное расследование по фактам разглашения, утечки информации и несанкционированного доступа к ней (ПК-17-1-2у.С3.ДВ.01.2);			+	+	
– организовывать и проводить аналитическую работу по предупреждению утечки конфиденциальной информации (ПК-17-1-3у.С3.ДВ.01.2).			+	+	
Владеет:					
– навыками выбора метода определения ущерба, наносимого владельцу информации в результате противоправного ее использования (ПК-5-2-1в.С3.ДВ.01.2);			+	+	
– навыками работы с персоналом, принятия организационно-управленческих решений, в том числе в нестандартных ситуациях в целях обеспечения информационной безопасности в организациях (ПК-12-1-1в.С3.ДВ.01.2);			+	+	
– организации доступа к объектам информатизации и обеспечения режима секретности, организации и управления деятельностью службы защиты информации в организациях (ПК-17-1-1в.С3.ДВ.01.2).			+	+	

ТО – текущий опрос (контроль знаний по теме);

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

ОПЗ – отчет по практическому заданию на групповых занятиях (оценка умений и владений);

ОИЗМ – отчет по выполнению индивидуального задания по модулю (оценка умений и владений);

Экз. – (оценка знаний).

7 График учебного процесса по дисциплине

Таблица 7.1 – График учебного процесса по дисциплине

Виды работ	**Распределение часов по учебным неделям**																		Итого, ч
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	
Раздел:	**1**						**2**					**3**							
Лекции	2	2	2	2	2	2	2	2	2	2		2	2	2	2	2	2		**32**
Практические, семинарские занятия (ПЗ, СЗ)			2	2	2	2	2	2	2	2	2	2	2	2	2	4	2	4	**36**
Самост. изучение теоретического материала		2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	4	**36**
Вып. инд. заданий (ИЗМ)		2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	4	**36**
КСР							1					1						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

Внутренний аудит систем защиты информации на соответствие стандартам	***Профессиональный цикл***
(*полное название дисциплины*)	(*цикл дисциплины*)
	основная
x	по выбору студента
	базовая часть цикла
x	вариативная часть цикла

090303.65/09030307.65	**Информационная безопасность автоматизированных систем»** специализация «Обеспечение информационной безопасности распределенных информационных систем»
(*код направления / специальности*)	(*полное название направления подготовки / специальности*)

КОБ/КОБ	Уровень подготовки	x	специалист	Форма обучения	x	очная
			бакалавр			заочная
			магистр			очно-заочная
(*аббревиатура направления / специальности*)						

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

Зорин Александр Александрович, доцент,
электротехнический факультет,
кафедра АТ, телефон: 239-18-16.

СПИСОК ИЗДАНИЙ

№	Библиографическое описание (автор, заглавие, вид издания, место, издательство, год издания, количество страниц)	Количество экземпляров в библиотеке
1	2	3
1 Основная литература		
1	Ахметова С. Г. Информационная безопасность: учебно-методическое пособие; Пермский национальный исследовательский политехнический университет. – Пермь: Изд-во ПНИПУ, 2013. – 122 с.	6 + ЭБ
2	Гафнер В. В. Информационная безопасность: учебное пособие для вузов. – Ростов-на-Дону: Феникс, 2010. – 324 с.	2
3	Информационная безопасность и защита информации: учебное пособие для вузов / Громов Ю. Ю. и др. – Старый Оскол: ТНТ, 2010. – 383 с.	5
	Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей: учебное пособие. – М: ФОРУМ: ИНФРА-М, 2009. – 415 с.	2
2 Дополнительная литература		
	2.1 Учебные и научные издания	
1	Манилов В.Л. Безопасность в эпоху партнерства. - М: ТЕРРА, 1999. – 363 с.	1
2	Возженников А.В., Кривельская Н.В., Макаренко И.В. Общая теория национальной безопасности: Учеб.; под. ред. Прохожева А.А.— М: РАГС, 2005. – 318 с.	3
3	Ярочкин В. И. Информационная безопасность: учебник для вузов, 5-е изд. - М: Акад. проект, 2008. – 543 с.	21
	2.2 Периодические издания	
	Не используются	

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

Не предусмотрены

8.3 Программные инструментальные средства

Не предусмотрены

8.4 Аудио- и видео-пособия

Не предусмотрены

8.5 Интернет-ресурсы

Таблица 8.5 – Используемые «Интернет-ресурсы»

№ п/п	Вид учебного занятия	Наименование «Интернет-ресурса»	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

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	308 корп. А	34	18

9.2 Основное учебное оборудование

Таблица 9.2 – Учебное оборудование

№ п.п.	Наименование и марка оборудования (стенда, макета, плаката)	Кол-во, ед.	Форма приобретения / владения (собственность, оперативное управление, аренда и т.п.)	Номер аудитории
1	ПК Intel Pentium Dual CPU 2000 МГц	6	Оперативное управление	308 корп. А

Лист регистрации изменений

№ п.п.	Содержание изменения	Дата, номер протокола заседания кафедры. Подпись заведующего кафедрой
1	2	3
1		
2		
3		
4		

УОП 3+

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__» ___01___ 2017 г. № 18

УЧЕБНО-МЕТОДИЧЕСКИЙ КОМПЛЕКС ДИСЦИПЛИНЫ
«Внутренний аудит систем защиты информации на соответствие стандартам»
РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Специальность:	10.05.03 Информационная безопасность автоматизированных систем
Специализация программы специалитета:	Обеспечение информационной безопасности автоматизированных систем
Квалификация выпускника:	специалист по защите информации
Выпускающая кафедра:	Автоматика и телемеханика
Форма обучения:	очная

Курс: 4 **Семестр: 8**
Трудоемкость:
Кредитов по базовому учебному плану (БУП): **5**
Часов по базовому учебному плану (БУП): **180**

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

Пермь 2017 г.

Рабочая программа дисциплины «Внутренний аудит систем защиты информации на соответствие стандартам» 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:

Теория систем массового обслуживания. Разработка и эксплуатация защищенных автоматизированных систем. Защита и обработка конфиденциальных документов. Метрология, стандартизация и сертификация. Организация и управление службой защиты информации на предприятии. Аудит информационной безопасности.

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» 01. 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, 5-8, 9-14, 28-35) внесены на основании перехода на ФГОС ВО по направлению подготовки (специальности) 10.05.03 Информационная безопасность автоматизированных систем (квалификация (степень) «специалист»), утвержденного приказом Министерства образования и науки Российской Федерации от «01» декабря 2016 г. № 1509; - профессиональную компетенцию ПК-12 считать профессиональной компетенцией **ПК-3,** с формулировкой «способность проводить анализ защищенности автоматизированных систем»; - изменить шифр дисциплинарной компетенции с ПК-12. С3.ДВ.01.2 на ПК-3. Б1.ДВ.04.2; - профессиональную компетенцию **ПК-6** считать объединением профессиональных компетенций ПК-5, ПК-17 с формулировкой «способность проводить анализ, предлагать и обосновывать выбор решений по обеспечению эффективного применения автоматизированных систем в сфере профессиональной деятельности»; - изменить шифры дисциплинарных компетенций с ПК-5. С3.ДВ.01.2, ПК-17. С3.ДВ.01.2 на ПК-6. Б1.ДВ.04.2.	
	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)».	
	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 5 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 4.4 «Распределение тем по видам самостоятельной работы» добавить параграф с наименованием «Методические указания для обучающихся по изучению дисциплины» следующего содержания: «При изучении дисциплины обучающимся целесообразно выполнять следующие рекомендации: 1. Изучение учебной дисциплины должно вестись систематически. 2. После изучения какого-либо раздела по учебнику или конспектным материалам рекомендуется по памяти воспроизвести основные термины, определения, понятия раздела. 3. Особое внимание следует уделить выполнению отчетов по практическим занятиям, лабораторным работам и индивидуальным комплексным заданиям на самостоятельную работу. 4. Изучение дисциплины осуществляется в течение одного семестра, график изучения дисциплины приводится п. 7. 5. Вся тематика вопросов, изучаемых самостоятельно, задается на лекциях преподавателем. Им же даются источники (в первую очередь вновь изданные в периодической научной литературе) для более детального понимания вопросов, озвученных на лекции.»	
	Наименование раздела 6 изложить в следующей редакции: «Фонд оценочных средств дисциплины».	
	Наименование параграфа 6.1 изложить в редакции «Текущий и рубежный контроль освоения заданных дисциплинарных частей компетенций».	
	В параграф 6.1 добавить первый абзац следующего содержания: «Текущий контроль осуществляется путем устного опроса во время аудиторных занятий».	
	Наименование раздела 8 Учебно-методическое и информационное обеспечение дисциплины» изложить в следующей редакции: «Перечень учебно-методического и информационного обеспечения для самостоятельной работы обучающихся по дисциплине».	
	Изменить название раздела «Список изданий» на «8.2. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины».	
	Добавить в таблицу 8.1 строку «2.5 Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины».	
	Дополнить п. 2.5 таблицы строками: **Электронная библиотека** Научной библиотеки Пермского	

	национального исследовательского политехнического университета [Электронный ресурс : полнотекстовая база данных электрон. документов изданных в Изд-ве ПНИПУ]. – Электрон. дан. (1 912 записей). – Пермь, 2014. – Режим доступа: http://elib.pstu.ru/. – Загл. с экрана. **Лань** [Электронный ресурс : электрон.-библ. система : полнотекстовая база данных электрон. документов по гуманит., естеств., и техн. наукам] / Изд-во «Лань». – Санкт-Петербург : Лань, 2010- . – Режим доступа: http://e.lanbook.com/. – Загл. с экрана. **Консультант Плюс** [Электронный ресурс : справочная правовая система : документы и комментарии : универсал. информ. ресурс]. – Версия Проф, сетевая. – Москва, 1992. – Режим доступа: Компьютер. сеть Науч. б-ки Перм. нац. исслед. политехн. ун-та, свободный.».	
	Раздел 8.2 «Компьютерные обучающие и контролирующие программы» считать раздел 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 раздел 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.		