

Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего профессионального образования



**Пермский национальный исследовательский
политехнический университет**

Электротехнический факультет
Кафедра «Автоматика и телемеханика»



УТВЕРЖДАЮ

Проректор по учебной работе

Н. В. Лобов

2015 г.

**УЧЕБНО-МЕТОДИЧЕСКИЙ КОМПЛЕКС ДИСЦИПЛИНЫ
«Аудит информационной безопасности»**

Основная образовательная программа подготовки специалистов
Специальность: 090303.65 «Информационная безопасность автоматизирован-
ных 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(ы): 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 «Аудит информационной безопасности» разработана на основании:

- федерального государственного образовательного стандарта высшего профессионального образования утвержденного приказом Министерства образования и науки Российской Федерации от 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: Организация и управление службой защиты информации на предприятия, Основы информационной безопасности, Управление информационной безопасностью.

Разработчик доцент

 Саранин Е.И.

Рецензент канд. техн. наук, доцент

 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

«06» 10 2015г., протокол № 44

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 в системе защиты информации на основе организации и проведения аудита информационной безопасности.

В процессе изучения данной дисциплины студент осваивает следующие дисциплинарные компетенции:

- способность применять методологию научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами (ПК-5);
- способность осуществлять поиск, изучение, обобщение и систематизацию научно-технической информации, нормативных и методических материалов в сфере своей профессиональной деятельности (ПК-9);
- способность проводить анализ защищенности автоматизированных систем (ПК-12).

1.2 Задачи дисциплины:

изучение:

- основных понятий аудита информационной безопасности;
- процессного подхода к организации информационной безопасности;
- основных требований к содержанию аудита информационной безопасности;
- основ контроля и проверки процессов и систем;
- процесса комплексного обследования информационной безопасности;
- методов оценивания информационной безопасности;

формирование умений:

- оценивания информационной безопасности на основе показателей информационной безопасности;
- исследования полученных оценок информационной безопасности;

овладение навыками использования методологии, стандартов и нормативных требований в области аудита информационной безопасности.

1.3 Предметом освоения дисциплины являются следующие объекты:

- процессный подход и информационная безопасность;
- циклическая модель менеджмента качества процессов и систем;
- способы и цели контроля и проверки процессов и систем;
- роли и обязанности по проведению оценивания;
- модель оценки процесса;
- внутренний и внешний аудит;
- правовые и методологические основы аудита информационной безопасности;
- система обеспечения информационной безопасности;
- методы оценивания информационной безопасности;
- особенности аудита информационной безопасности организаций банковской системы Российской Федерации;
- направления обеспечения и оценки информационной безопасности;
- особенности аудита информационной безопасности организаций, использующих аутсорсинг.

1.4 Место дисциплины в структуре профессиональной подготовки выпускников.

Дисциплина «Аудит информационной безопасности» относится к вариативной части цикла профессиональных дисциплин и является дисциплиной по выбору 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 понятия аудита информационной безопасности;
- процессный подход к организации информационной безопасности;
- содержание циклической модели менеджмента качества процессов и систем;
- правовые и методологические основы аудита информационной безопасности;
- международные правовые аспекты, стандарты и руководства по основам аудита информационной безопасности;
- основные требования к содержанию аудита информационной безопасности;
- основы контроля и проверки процессов и систем;
- содержание процесса комплексного обследования информационной безопасности;
- методы оценивания информационной безопасности;
- направления обеспечения и оценки информационной безопасности.

уметь:

- использовать международные правовые аспекты, стандарты и руководства по основам аудита информационной безопасности;
- оценивать информационную безопасность на основе показателей информационной безопасности;
- исследовать полученные оценки информационной безопасности;
- оценивать результаты аудита и самооценки информационной безопасности;

владеть:

- навыками использования методологии, стандартов и нормативных требования в области аудита информационной безопасности;
- навыками разработки и исследования процессов защиты информации и ее компонентов по результатам аудита информационной безопасности.

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

Индекс	Наименование компетенции	Предшествующие дисциплины	Последующие дисциплины (группы дисциплин)
Профессиональные компетенции			
ПК-5	способность применять методологию научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами	Организация и управление службой защиты информации на предприятии	Подготовка и защита ВКР

ПК-9	способность осуществлять поиск, изучение, обобщение и систематизацию научно-технической информации, нормативных и методических материалов в сфере своей профессиональной деятельности	Основы информационной безопасности	Междисциплинарный государственный экзамен
ПК-12	способность проводить анализ защищенности автоматизированных систем	Управление информационной безопасностью	Преддипломная практика

2 Требования к результатам освоения учебной дисциплины

Учебная дисциплина обеспечивает формирование заданных частей профессиональных компетенций (ПК-5, ПК-9 и ПК-12).

2.1 Карты дисциплинарных компетенций

2.1.1 Карта дисциплинарной компетенции ПК-5

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

Индекс ПК-5-4	Формулировка дисциплинарной части компетенции: способен применять методологию научных исследований в вопросах организации и проведения аудита информационной безопасности
----------------------	---

2.1.2 Компонентный состав дисциплинарной компетенции

Перечень компонентов	Виды учебной работы	Средства контроля
Знать: – основные понятия аудита информационной безопасности (ПК-5-4-1з); – процессный подход к организации информационной безопасности (ПК-5-4-2з); – содержание циклической модели менеджмента качества процессов и систем (ПК-5-4-3з); – правовые и методологические основы аудита информационной безопасности (ПК-5-4-4з);	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
Уметь: – использовать международные правовые аспекты, стандарты и руководства по основам аудита информационной безопасности (ПК-5-4-1у); – оценивать информационную безопасность на основе показателей информационной безопасности (ПК-5-4-2у);	Практические занятия; выполнение индивидуального задания.	Защита отчета по выполнению индивидуального задания.

Владеть: – навыками использования методологии, стандартов и нормативных требования в области аудита информационной безопасности (ПК-5-4-1в).	Выполнение индивидуального комплексного задания.	Защита отчета по индивидуальному комплексному заданию.
--	--	--

2.2.1 Карта дисциплинарной компетенции ПК-9

Индекс ПК-9	Формулировка компетенции: способность осуществлять поиск, изучение, обобщение и систематизацию научно-технической информации, нормативных и методических материалов в сфере своей профессиональной деятельности
--------------------	---

Индекс ПК-9-7	Формулировка дисциплинарной части компетенции: способность осуществлять поиск, изучение, обобщение и систематизацию научно-технической информации, нормативных и методических материалов в вопросах организации и проведения аудита информационной безопасности
----------------------	---

2.2.2 Компонентный состав дисциплинарной компетенции

Перечень компонентов	Виды учебной работы	Средства контроля
Знать: – международные правовые аспекты, стандарты и руководства по основам аудита информационной безопасности (ПК-9-7-1з); – основные требования к содержанию аудита информационной безопасности (ПК-9-7-2з); – основы контроля и проверки процессов и систем (ПК-9-7-3з);	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
Уметь: – исследовать полученные оценки информационной безопасности (ПК-9-7-1у); – оценивать результаты аудита и самооценки информационной безопасности (ПК-9-7-2у);	Практические занятия; выполнение индивидуального задания.	Защита отчета по выполнению индивидуального задания.
Владеть: – навыками разработки процессов защиты информации и ее компонентов по результатам аудита информационной безопасности (ПК-9-7-1в).	Выполнение индивидуального задания.	Защита отчета по выполнению индивидуального задания.

2.2.1 Карта дисциплинарной компетенции ПК-12

Индекс ПК-12	Формулировка компетенции: способен проводить анализ защищенности автоматизированных систем
---------------------	--

Индекс ПК-12-2	Формулировка дисциплинарной части компетенции: способен проводить анализ защищенности автоматизированных систем при проведении аудита информационной безопасности
-----------------------	---

2.2.2 Компонентный состав дисциплинарной компетенции

Перечень компонентов	Виды учебной работы	Средства контроля
Знать: – содержание процесса комплексного обследования информационной безопасности (ПК-12-2-1з);	Лекции; семинарские и практические занятия; са-	Экзамен, отчет по выполнению практических задач, обсуж-

– методы оценивания информационной безопасности (ПК-12-2-2з); – направления обеспечения и оценки информационной безопасности (ПК-12-2-3з);	самостоятельное изучение теоретического материала.	защита результатов самостоятельного изучения теоретического материала в ходе ПЗ и СЗ
Уметь: – исследовать полученные оценки информационной безопасности (ПК-12-2-1у); – оценивать результаты аудита и самооценки информационной безопасности (ПК-12-2-2у);	Практические занятия; выполнение индивидуального задания.	Защита отчета по выполнению индивидуального задания.
Владеть: – навыками исследования процессов защиты информации и ее компонентов по результатам аудита информационной безопасности (ПК-12-2-1в).	Выполнение индивидуального задания.	Защита отчета по выполнению индивидуального задания.

3. Структура учебной дисциплины по видам и формам учебной работы

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

3.2. Основными видами аудиторной работы по дисциплине являются:

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

3.3. Основными видами самостоятельной работы по дисциплине являются:

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

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

Таблица 3.1 – Структура дисциплины по объемам 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	32	
	- 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)	180	
	в зачётных единицах (ЗЕ)	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)							Итог. аттест.	Трудоёмкость АЧ/ЗЕТ
			Аудиторная работа студента (АРС)				Самостоятельная работа студента (СРС)				
			Всего	Лк	ПЗ, СЗ	КСР	Всего	ИТМ	ИЗМ		
1	2	3	4	5	6	7	8	9	10	11	12
1	1	1	4	2	2		4	2	2		8
		2	6	2	4		4	2	2		10
		3	8	4	4		8	4	4		16
		4	9	4	4	1	8	4	4		17
		Всего по модулю:	27	12	14	1	24	12	12		51
2	2	5	6	4	2		8	4	4		14
		6	6	2	4		8	4	4		14
		7	7	2	4	1	8	4	4		15
		Всего по модулю:	19	8	10	1	24	12	12		43
3	3	8	4	2	2		4	2	2		8
		9	4	2	2		4	2	2		8
		10	4	2	2		4	2	2		8
		11	4	2	2		4	2	2		8
		12	10	4	4	2	8	4	4		18
Всего по модулю:	26	12	12	2	24	12	12		50		
Итоговая аттестация											36
Итого			72	32	36	4	72	36	36	36	180/5

4.2. Содержание разделов и тем учебной дисциплины

Модуль 1. Основы аудита информационной безопасности

Раздел I. Основы аудита информационной безопасности

АРС: Л - 12 ч.; ПЗ (СЗ) - 14 ч., КСР – 2 ч., СРС: ИТМ - 12 ч., ИЗМ (ИЗМ-1) - 12 ч.

Тема 1. Введение в дисциплину. 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 другими дисциплинами учебного плана. Методические материалы и периодические издания. Обязательная и дополнительная литература.

Тема 2. Основы организации аудиторской деятельности. Основные понятия, термины и определения. Цели и задачи организации аудиторской деятельности. Причины организации аудита. Основные проблемы и задачи совершенствования аудиторской деятельности.

Тема 3. Аудит информационной безопасности как инструмент обеспечения информационной безопасности в современных условиях. Процессы и системы. Структура и свойства процессов и систем. Процессный подход и информационная безопасность. Циклическая модель менеджмента качества процессов и систем. Способы контроля и проверки процессов и систем. Цели контроля и проверки процессов и систем.

Тема 4. Нормативно-правовое обеспечение аудиторской деятельности. Исторические аспекты организации аудиторской деятельности. Международные нормы организации и

проведения аудиторской деятельности. Требования нормативных документов российской Федерации по организации аудита. Международные и внутриведомственные требования по организации аудита.

Модуль 2. Требования к содержанию аудита информационной безопасности организаций и систем

Раздел II. Требования к содержанию аудита информационной безопасности организаций и систем

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

Тема 5. Основы контроля и проверки процессов и систем. Определение входных данных оценки. Роли и обязанности по проведению оценивания. Модель оценки процесса. Мероприятия процесса оценивания и выходные данные оценивания. Факторы успешной оценки процесса. Внутренний и внешний аудит. Модели безопасности бизнеса.

Тема 6. Аудит информационной безопасности организаций и систем. Правовые и методологические основы аудита информационной безопасности. Международные правовые аспекты, стандарты и руководства по основам аудита информационной безопасности. Национальные стандарты и руководства по основам аудита информационной безопасности. Отечественные законы и стандарты по основам аудита информационной безопасности..

Тема 7. Осознание и менеджмент аудита информационной безопасности. Система обеспечения информационной безопасности как совокупность процессов осознания и менеджмента информационной безопасности. Осознание аудита информационной безопасности.

Модуль 3. Особенности проведения аудита в комплексной системе обеспечения информационной безопасности

Раздел 3. Особенности проведения аудита в комплексной системе обеспечения информационной безопасности

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

Тема 8. Планирование аудита информационной безопасности. Планирование программы аудита информационной безопасности. Реализация программы аудита информационной безопасности. Контроль и совершенствование программы аудита информационной безопасности.

Тема 9. Оценивание информационной безопасности. Методы оценивания информационной безопасности. Оценивание информационной безопасности на основе показателей информационной безопасности. Оценивание информационной безопасности на основе моделей зрелости процессов обеспечения информационной безопасности.

Тема 10. Исследование результатов оценивания информационной безопасности. Исследование полученных оценок информационной безопасности. Оценивание результатов аудита и самооценки информационной безопасности. Оценивание процессов проведения аудита и самооценки информационной безопасности. Риск-ориентированная интерпретация полученных оценок информационной безопасности.

Тема 11. Практика аудита информационной безопасности организаций и систем. Особенности аудита информационной безопасности организаций банковской системы РФ. Особенности развития средств и систем автоматизации. Направления обеспечения и оценки информационной безопасности. Размерность и значимость объектов оценки при проведении аудита информационной безопасности. Работы по созданию системы оценки информационной безопасности организаций банковской системы Российской Федерации.

Тема 12. Аудит управления непрерывностью бизнеса и восстановления после сбоев. Методологии, стандарты и нормативные требования в области управления непрерывностью бизнеса. Основные цели аудита. Основные вопросы, рассматриваемые при аудите управления непрерывностью бизнеса и восстановления после сбоев. Реализация аудита. За-

ключительные процедуры аудита. Особенности аудита информационной безопасности организаций, использующих аутсорсинг.

4.3. Перечень тем практических занятий

Таблица 4.4 – Темы практических занятий (семинаров)

№ п/п	Номер темы дисциплины	Наименование темы практического (семинарского) занятия
1	1	Особенности формирования терминологии научной дисциплины
2	2	Основы контроля и проверки процессов и систем
3	3	Основные проблемы и задачи совершенствования аудиторской деятельности
4	4	Нормативно-правовое обеспечение аудиторской деятельности
5	5	Модели безопасности бизнеса (ПЗ)
6	6	Отечественные законы и стандарты по основам аудита информационной безопасности
7	7	Осознание аудита информационной безопасности
8	7	Менеджмент аудита информационной безопасности
9	8	Планирование программы аудита информационной безопасности (ПЗ)
10	9	Методы оценивания информационной безопасности (ПЗ)
11	10	Оценивание процессов проведения аудита и самооценки информационной безопасности
12	11	Размерность и значимость объектов оценки при проведении аудита информационной безопасности
13	12	Аудит управления непрерывностью бизнеса (ПЗ)
14	12	Аудит управления восстановлением после сбоев (ПЗ)

4.4. Перечень тем лабораторных работ

Не предусмотрены.

4.5 Виды самостоятельной работы студентов

Таблица 4.5 – Виды самостоятельной работы студентов (СРС)

Номер темы (раздела) дисциплины	Вид самостоятельной работы студентов	Трудоемкость, часов
1	ИТМ: Аудит информационной безопасности как инструмент обеспечения информационной безопасности в современных условиях	2
2	ИТМ: Определение входных данных оценки процессов и систем	2
3	ИТМ: Цели контроля и проверки процессов и систем	4
4	ИТМ: Способы контроля и проверки процессов и систем	4
4	ИЗМ: В соответствии с заданием для модуля 1, п.п. 4.5.1	12
5	ИТМ: Модели безопасности бизнеса	4
6	ИТМ: Аудит информационной безопасности организаций и систем	4
7	ИТМ: Отечественные законы и стандарты по основам аудита	4

7	ИЗМ: В соответствии с заданием для модуля 2, п.п. 4.5.1	12
8	ИТМ: Осознание аудита информационной безопасности	2
9	ИТМ: Риск-ориентированная интерпретация полученных оценок информационной безопасности	2
10	ИТМ: Работы по созданию системы оценки информационной безопасности организаций банковской системы Российской Федерации	2
11	ИТМ: Аудит управления непрерывностью бизнеса и восстановления после сбоев	2
12	ИТМ: Особенности аудита информационной безопасности организаций, использующих аутсорсинг	4
12	ИЗМ: В соответствии с перечнем тем для модуля 3, п.п. 4.5.1	12
Итого: в ч / в ЗЕ		72/2

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

Индивидуальное задание представляет собой разрабатываемый студентом отчет по вопросам организации и управления службой защиты информации на предприятии. Темы изучаются студентом самостоятельно, в течение всего учебного семестра и отражает необходимые требования по основным задачам, решаемым в процессе организации и управления подразделением, обеспечивающим информационную безопасность предприятия. Последовательность разработки тем осуществляется поэтапно, в соответствии с последовательностью изучаемых разделов учебной дисциплины.

Раздел 1, модуль 1

- Тема 1.** Структура и свойства процессов и систем.
- Тема 2.** Процессный подход и информационная безопасность.
- Тема 3.** Циклическая модель менеджмента качества процессов и систем.
- Тема 4.** Способы контроля и проверки процессов и систем.

Раздел 2, модуль 2

- Тема 5.** Роли и обязанности по проведению оценивания.
- Тема 6.** Факторы успешной оценки процесса.
- Тема 7.** Международные правовые аспекты, стандарты и руководства по основам аудита информационной безопасности.

Раздел 3, модуль 3

- Тема 8.** Оценивание информационной безопасности на основе показателей информационной безопасности.
- Тема 9.** Оценивание информационной безопасности на основе моделей зрелости процессов обеспечения информационной безопасности.
- Тема 10.** Исследование полученных оценок информационной безопасности.
- Тема 11.** Оценивание результатов аудита и самооценки информационной безопасности.
- Тема 12.** Особенности развития средств и систем автоматизации аудита.

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 и нормативно-методических документов по организации и проведению аудита информационной безопасности, рекомендаций по применению современных методов и средств защиты информации.

6. Управление и контроль освоения компетенций

6.1 Текущий контроль освоения заданных дисциплинарных компетенций

Текущий контроль освоения дисциплинарных компетенций проводится в следующих формах:

- текущий опрос, текущая проверочная работа для анализа усвоения материала предыдущей лекции (ТО);
- оценка работы студента на лекционных, практических и семинарских занятиях в рамках рейтинговой системы.

6.2 Рубежный и промежуточный контроль освоения заданных дисциплинарных компетенций

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

- отчет за индивидуальное задание по модулю (модуль 1, 2, 3);
- тест для рубежного контроля (модуль 1, 2, 3) (РТ).

6.3 Итоговый контроль освоения заданных дисциплинарных компетенций

1) Экзамен

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

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

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

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

Таблица 6.1 - Виды контроля освоения элементов и частей компетенций

Контролируемые результаты освоения дисциплины (ЗУВы)	Вид/форма контроля				
	ТО	РТ	ОПЗ	ОИЗМ	Экз.
В результате освоения дисциплины студент					
Знает:					
– основные понятия аудита информационной безопасности (ПК-5-4-1з);	+	+	+		+
– процессный подход к организации информационной безопасности (ПК-5-4-2з);	+	+	+		+
– содержание циклической модели менеджмента качества процессов и систем (ПК-5-4-3з);	+	+	+		+
– правовые и методологические основы аудита информационной безопасности (ПК-5-4-4з);	+	+	+		+
– международные правовые аспекты, стандарты и руководства по основам аудита информационной безопасности (ПК-9-7-1з);	+	+	+		+
– основные требования к содержанию аудита информационной безопасности (ПК-9-7-2з);	+	+	+		+
– основы контроля и проверки процессов и систем (ПК-9-7-3з);	+	+	+		+
– содержание процесса комплексного обследования информационной безопасности (ПК-12-2-1з);	+	+	+		+
– методы оценивания информационной безопасности (ПК-12-2-2з);	+	+	+		+
– направления обеспечения и оценки информационной безопасности (ПК-12-2-3з);	+	+	+		+
Умеет:					
– использовать международные правовые аспекты, стандарты и руководства по основам аудита информационной безопасности (ПК-5-4-1у);			+	+	
– оценивать информационную безопасность на основе показателей информационной безопасности (ПК-5-4-2у);			+	+	
– исследовать полученные оценки информационной безопасности (ПК-9-7-1у);			+	+	
– оценивать результаты аудита и самооценки информационной безопасности (ПК-9-7-2у);			+	+	
– исследовать полученные оценки информационной безопасности (ПК-12-2-1у);			+	+	
– оценивать результаты аудита и самооценки информационной безопасности (ПК-12-2-2у);			+	+	
Владеет:					
– навыками использования методологии, стандартов и нормативных требования в области аудита информационной безопасности (ПК-5-4-1в);			+	+	
– навыками разработки процессов защиты информации и ее компонентов по результатам аудита информационной безопасности (ПК-9-7-1в);			+	+	
– навыками исследования процессов защиты информации и ее компонентов по результатам аудита информационной безопасности (ПК-12-2-1в).			+	+	

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	2	2	2	2	2	36
Самост. изучение теоретического материала	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	36
Вып. инд. заданий (ИЗМ)	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	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

Аудит информацион- ной безопасности
--

полное название дисциплины

Профессиональный цикл

x

обязат.
по выбору
студента

x

базовая часть
цикла
вариативная
часть цикла

090303.65

*код направления / специаль-
ности*

«Информационная безопасность автоматизирован- ных систем», специализация «Обеспечение информаци- онной безопасности распределенных информационных систем»
--

полное название направления/ специальности

КОБ/КОБ

Уровень
подготовки

x	специалист
	бакалавр
	магистр

Форма
обучения

x	очная
	заочная
	очно-заочная

2015

семестр(ы) 8

количество групп
количество студентов

1
20

Саранин Евгений Ильич, доцент,
электротехнический факультет,
кафедра АТ, телефон: 239-18-16.

Карта книго-
обеспеченности
в библиотеку сдана

СПИСОК ИЗДАНИЙ

№	Библиографическое описание	Количество экземпляров в библиотеке
1	2	3
1. Основная литература		
1	Миргородская Т. В. Аудит : учебное пособие для вузов / Т. В. Миргородская .— 3-е изд., перераб. и доп .— Москва : КНОРУС, 2011 .— 281 с., 2014-2015, Лань "	40
2	Анисимов А.А. Менеджмент в сфере информационной безопасности: учебное пособие / А. А. Анисимов ; Интернет-университет информационных технологий .— Москва : ИНГУИТ : БИНОМ. Лаб. знаний, 2010 .— 175 с.	2
3	Основы управления информационной безопасностью : учебное пособие для вузов / А. П. Курило [и др.] .— 2-е изд., испр.— Москва : Горячая линия-Телеком, 2014 .— 243 с.	15
2. Дополнительная литература		
2.1. Учебные и научные издания		
1	Юдина Г. А. Основы аудита : учебное пособие для вузов / Г. А. Юдина, М. Н. Черных .— 5-е изд., перераб. и доп .— Москва : КНОРУС, 2012 .— 383 с.,	1
2	Фатхутдинов Р. А. Управленческие решения : учебник для вузов / Р. А. Фатхутдинов .— 6-е изд., перераб. и доп .— Москва : ИНФРА-М, 2009 .— 343 с.	5
3	Васин С. М. Управление рисками на предприятии : учебное пособие для вузов / С.М. Васин, В.С. Шутов .— Москва : КНОРУС, 2010 .— 299 с.: ил. — Библиогр.: с. 298-299 .	7

Основные данные об обеспеченности на _____

(дата составления рабочей программы)

Основная литература

обеспечена

не обеспечена

Дополнительная литература

обеспечена

не обеспечена

Зав. отделом комплектования
научной библиотеки

Н. В. Тюрикова

Текущие данные об обеспеченности на _____

(дата контроля литературы)

Основная литература

обеспечена

не обеспечена

Дополнительная литература

обеспечена

не обеспечена

Зав. отделом комплектования
научной библиотеки

Н.В. Тюрикова

Карта книго-
обеспеченности
в библиотеку сдана

8.2 Компьютерные обучающие и контролирующие программы

Таблица 8.1 – Используемые компьютерные обучающие программы

№ п/п	Вид учебного занятия	Наименование программного продукта	Рег. номер	Назначение
1	2	3	4	5
1	ПЗ, СЗ	Базы данных правовой информации – Информационно-правового обеспечения “Гарант” - www.garant.ru; – Справочно-правовой системы “Консультант Плюс” - www.consultant.ru.	б/н	

8.3 Программные инструментальные средства

Презентационные материалы для лекционных занятий

8.4 Аудио- и видео-пособия

Не предусмотрены

9 Материально-техническое обеспечение дисциплины

9.1 Специализированные лаборатории и классы

Таблица 9.1 – Специализированные лаборатории и классы

№ п.п.	Помещения			Площадь, м ²	Количество посадочных мест
	Название	Принадлежность (кафедра)	Номер аудитории		
1	2	3	4	5	6
1	Дисплейный класс	Кафедра АТ	308 корп. А	34	18

9.2 Основное учебное оборудование

Таблица 9.2 – Учебное оборудование

№ п.п.	Наименование и марка оборудования (стенда, макета, плаката)	Кол-во, ед.	Форма приобретения / владения (собственность, оперативное управление, аренда и т.п.)	Номер аудитории
1	2	3	4	5
1	ПК Intel Pentium Dual CPU 2000 МГц	6	Оперативное управление	308 корп. А

Лист регистрации изменений

№ п.п.	Содержание изменения	Дата, номер протокола заседания кафед- ры
1.		
2.		
3.		
4.		
5.		

Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования



**«Пермский национальный исследовательский
политехнический университет»
Электротехнический факультет
Кафедра «Автоматика и телемеханика»**

УТВЕРЖДАЮ
Заведующий кафедрой
«Автоматика и телемеханика»
д-р техн. наук, проф.
_____ А.А. Южаков
Протокол заседания кафедры АТ
от « 16 » _____ 01 _____ 2017 г. № 18

**УЧЕБНО-МЕТОДИЧЕСКИЙ КОМПЛЕКС ДИСЦИПЛИНЫ
«Аудит информационной безопасности»
РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ**

Специальность:	10.05.03 Информационная безопасность автоматизированных систем
Специализация программы специалитета:	Обеспечение информационной безопасности распределенных информационных 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: - **нет** Курсовой проект: - **нет** Курсовая работа: - **нет**

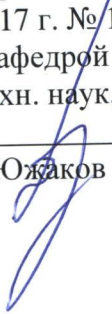
Пермь 2017 г.

Рабочая программа дисциплины «Аудит информационной безопасности» 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: Защита и обработка конфиденциальных документов, Информационная безопасность в банковской системе, Внутренний аудит систем защиты информации на соответствие стандартам, Организация и управление службой защиты информации на предприятии, Методы проектирования защищенных распределенных информационных систем базового учебного плана образовательной программы высшего образования - программы по специальности 10.05.03 Информационная безопасность автоматизированных систем, специализации Обеспечение информационной безопасности распределенных информационных систем.

Лист регистрации изменений

№ п.п	Содержание изменения	Дата, номер протокола заседания кафедры. Подпись заведующего кафедрой
1.	<p>Содержание стр. 1, кроме абзацев 6-9, изложить в редакции, приведенной на стр. 1а.</p> <p>Содержание стр. 2 (абзацы 1-5) изложить в редакции, приведенной на стр. 2а.</p> <p>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;</p> <ul style="list-style-type: none"> - объединение профессиональных компетенций ПК-5 и ПК-9 считать профессиональной компетенцией ПК-3, с формулировкой «Способностью проводить анализ защищенности автоматизированных систем»; - изменить шифр дисциплинарных компетенций с ПК-5.С3.ДВ.3.2 и ПК-9.С3.ДВ.3.2 на ПК-3.Б1.ДВ.06.2 - профессиональную компетенцию ПК-12 считать профессиональной компетенцией ПСК-7.3 с формулировкой «Способностью проводить аудит защищенности информационно-технологических ресурсов распределенных информационных систем»; - изменить шифр дисциплинарной компетенции с ПК-12.С3.ДВ.3.2 на ПСК- 7.3.Б1.ДВ.06.2 <p>Наименование раздела 1.4 «Место учебной дисциплины в структуре профессиональной подготовки выпускников» изложить в следующей редакции: «Место учебной дисциплины в структуре образовательной программы».</p> <p>В первом абзаце раздела 1.4 заменить слова «цикла профессиональных дисциплин» на «блока 1. Дисциплины (модули)».</p> <p>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».</p> <p>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.».</p>	<p>Протокол заседания кафедры АТ от «16» 01. 2017 г. №18 Зав. кафедрой АТ д-р техн. наук, проф.</p> <p>_____</p> <p>А.А. Южаков</p> 

<p>В табл. 3.1.:</p> <p>а) строку п. 1 дополнить словами «(контактная работа)»;</p> <p>б) строку п. 3 изложить в следующей редакции: «Итоговый контроль (промежуточная аттестация обучающихся) по дисциплине:».</p>	
<p>В табл. 4.1.:</p> <p>а) в строке п. 1 «Количество часов (очная форма обучения)» дополнить словами «и виды занятий»;</p> <p>б) «Итоговая аттестация» заменить на «Итоговый контроль (промежуточная аттестация).</p>	
<p>В раздел 4.4 «Распределение тем по видам самостоятельной работы» добавить параграф с наименованием «Методические указания для обучающихся по изучению дисциплины» следующего содержания:</p> <p>«При изучении дисциплины обучающимся целесообразно выполнять следующие рекомендации:</p> <ol style="list-style-type: none"> 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.» 	
<p>Наименование раздела 6 изложить в следующей редакции: «Фонд оценочных средств дисциплины».</p>	
<p>Наименование параграфа 6.1 изложить в редакции «Текущий и рубежный контроль освоения заданных дисциплинарных частей компетенций».</p>	
<p>В параграф 6.1 добавить первый абзац следующего содержания: «Текущий контроль осуществляется путем устного опроса во время аудиторных занятий».</p>	
<p>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».</p>	
<p>Изменить название раздела «Список изданий» на «8.2. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины».</p>	
<p>Добавить в таблицу 8.1 строку «2.5 Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины».</p>	
<p>Дополнить п. 2.5 таблицы строками: Электронная библиотека Научной библиотеки Пермского</p>	

	<p>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.</p> <p>Лань [Электронный ресурс : электрон.-библ. система : полнотекстовая база данных электрон. документов по гуманитар., естеств., и техн. наукам] / Изд-во «Лань». – Санкт-Петербург : Лань, 2010- . – Режим доступа: http://e.lanbook.com/. – Загл. с экрана.</p> <p>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.». </p> <p>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».</p> <p>Раздел 8.3 «Программные инструментальные средства» считать раздел 8.4 «Перечень программного обеспечения, в том числе компьютерные обучающие и контролирующие программы».</p> <p>Раздел 8.4 «Аудио- и видео-пособия» считать разделом 8.5.</p> <p>Наименование раздела 9 изложить в следующей редакции: «Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине».</p>	
2.		
3.		
4.		
5.		