Министерство образования и науки Российской Федерации

Федеральное государственное бюджетное образовательное учреждение
высшего профессионального образования

**Пермский национальный исследовательский
политехнический университет**

Электротехнический факультет
Кафедра автоматики и телемеханики

УТВЕРЖДАЮ
Проректор по учебной работе
д.р. техн. наук, проф.
_____ Н. В. Лобов
_____ 2015 г.

УНИФИЦИРОВАННЫЙ УЧЕБНО-МЕТОДИЧЕСКИЙ КОМПЛЕКС ДИСЦИПЛИНЫ
«Управление информационной безопасностью»

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Основная образовательная программа подготовки бакалавров и специалистов
по направлению: 090900.62 «Информационная безопасность»
по специальности: 090303.65 «Информационная безопасность автоматизированных систем»

Профиль подготовки бакалавра	- 09090003.62 Комплексная защита объектов информатизации
Специализация специалиста	- 09030307.65 Обеспечение информационной безопасности распределенных информационных систем
Квалификация (степень) выпускника	- бакалавр/ специалист
Специальное звание выпускника	- специалист по защите информации
Выпускающая кафедра	«Автоматика и телемеханика»
Форма обучения	очная

Курс: 4 **Семестр**: 7

Трудоёмкость:

Кредитов по рабочему учебному плану:	4	ЗЕ
Часов по рабочему учебному плану:	152	Ч

Виды контроля:

Экзамен: **- 7 сем.** Зачёт: - Курсовой проект: - Курсовая работа: -

Пермь 2015 г.

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

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

УЧЕБНО-МЕТОДИЧЕСКИЙ КОМПЛЕКС ДИСЦИПЛИНЫ
«Управление информационной безопасностью»
РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

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

Курс: 4 **Семестр:** 7

Трудоемкость:

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

Виды контроля:

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

Пермь 2017 г.

Рабочая программа дисциплины «Управление информационной безопасностью» разработана на основании:

- федерального государственного образовательного стандарта высшего профессионального образования, утвержденного приказом Министерства образования и науки Российской Федерации от «28» октября 2009 г., № 496, по направлению подготовки 090900 Информационная безопасность (квалификация (степень) «бакалавр»);
- федерального государственного образовательного стандарта высшего профессионального образования утвержденного приказом Министерства образования и науки Российской Федерации «17» января 2011г. № 60, по направлению подготовки (специальности) 090303 «Информационная безопасность автоматизированных систем» (квалификация (степень) «специалист»);
- компетентностной модели выпускника ООП по направлению подготовки 090900.62 - «Информационная безопасность», профилю подготовки «Комплексная защита объектов информатизации», утвержденной «24» июня 2013 г.;
- компетентностной модели выпускника ООП по специальности 090303.65 - «Информационная безопасность автоматизированных систем», специализации «Обеспечение информационной безопасности распределенных информационных систем», утвержденной «24» июня 2013 г.;
- базового учебного плана очной формы обучения по направлению подготовки 090900.62 - «Информационная безопасность», профилю подготовки «Комплексная защита объектов информатизации» «29» августа 2011 г.
- базового учебного плана очной формы обучения по специальности 090303.65 - «Информационная безопасность автоматизированных систем», специализации «Обеспечение информационной безопасности распределенных информационных систем», утвержденного «29» августа 2011 г.

Рабочая программа согласована с рабочей программой дисциплин: «Организационное и правовое обеспечение информационной безопасности», «Комплексная защита информации на предприятии».

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

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

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

Рабочая программа одобрена методической комиссией электротехнического факультета
«2» 02 2015г., протокол №30
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 «Управление информационной безопасностью» 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:

Безопасность систем баз данных, Безопасность операционных систем, Информационно-аналитическое обеспечение безопасности предприятия, Безопасность сетей ЭВМ базового учебного плана образовательной программы высшего образования - программы по специальности 10.05.03 Информационная безопасность автоматизированных систем, специализации Обеспечение информационной безопасности распределенных информационных систем.

1. Общие положения

1.1. Цель дисциплины - формирование компетентности в области основных понятий, методологии и практических приемов управления информационной безопасностью, технической и организационной инфраструктурой обеспечения информационной безопасности предприятия (организации).

В процессе изучения дисциплины студент осваивает следующие компетенции по направлениям подготовки ВПО:

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

№	Код направления/ специальности	Наименование направления/ специальности	Компетенции, формируемые на основе базовых учебных планов	
			Код компетенции	Формулировка компетенции
1.	090900.62	Информационная безопасность	ПК-9	способность принимать участие в эксплуатации подсистем управления информационной безопасностью предприятия
			ПСК-2	готовность к проведению анализа и оценки состояния защищенности объектов информатизации, на основе действующих международных и отечественных стандартов по защите информации
2.	090303.65	Информационная безопасность автоматизированных систем	ОК-6	способность к работе в коллективе, кооперации с коллегами, способностью в качестве руководителя подразделения, лидера группы сотрудников формировать цели команды, принимать организационно-управленческие решения в нестандартных ситуациях и нести за них ответственность, предупреждать и конструктивно разрешать конфликтные ситуации в процессе профессиональной деятельности
			ПК-21	способность участвовать в проектировании системы управления информационной безопасностью автоматизированной системы

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

Унифицированная профессиональная компетенция (УПК-1)

Способность принимать участие в эксплуатации подсистем управления информационной безопасностью предприятия, принимать организационно-управленческие решения в нестандартных ситуациях и нести за них ответственность

Унифицированная профессиональная компетенция (УПК-2)

Способность проводить анализ и оценку состояния защищенности объектов информатизации, участвовать в проектировании системы управления информационной безопасностью на основе действующих международных и отечественных стандартов по защите информации

Таблица 1.2 Обоснование разработки унифицированных компетенций

№	Направление подготовки		Соответствие унифицированной компетенции и базовой компетенции ФГОС ВПО	
	Код	Наименование	**Способность принимать участие в эксплуатации подсистем управления информационной безопасностью предприятия, принимать организационно-управленческие решения в нестандартных ситуациях и нести за них ответственность (УПК-1)**	**Способность проводить анализ и оценку состояния защищенности объектов информатизации, участвовать в проектировании системы управления информационной безопасностью на основе действующих международных и отечественных стандартов по защите информации (УПК-2)**
1.	090900.62	Информационная безопасность	Способность принимать участие в эксплуатации подсистем управления информационной безопасностью предприятия (ПК-9)	Готовность к проведению анализа и оценки состояния защищенности объектов информатизации, на основе действующих международных и отечественных стандартов по защите информации (ПСК-2)
2.	090303.65	Информационная безопасность автоматизированных систем	Способность к работе в коллективе, кооперации с коллегами, способностью в качестве руководителя подразделения, лидера группы сотрудников формировать цели команды, принимать организационно-управленческие решения в нестандартных ситуациях и нести за них ответственность, предупреждать и конструктивно разрешать конфликтные ситуации в процессе профессиональной деятельности (ОК-6)	Способность участвовать в проектировании системы управления информационной безопасностью автоматизированной системы (ПК-21)

1.2. Задачи дисциплины:

- определение целей и задач управления информационной безопасностью;
- изучение стандартов систем и процессов управления информационной безопасностью;
- освоение принципов формирования политики информационной безопасности;
- изучение и освоение основных методов управления информационной безопасностью;

- изучение методов оценки и обработки рисков, управления инцидентами информационной безопасности;
- освоение порядка организации аудита информационной безопасности;
- изучение принципов управления логическим доступом к активам организации, защищенной передачей данных, управления безопасностью информационных систем.

После изучения дисциплины обучающийся должен демонстрировать следующие результаты:

знать:

- цели и задачи управления информационной безопасностью;
- стандарты систем и процессов управления информационной безопасностью;
- принципы формирования политики информационной безопасности;
- основные методы управления информационной безопасностью;
- порядок оценки рисков информационной безопасности;
- методы обработки рисков информационной безопасности;
- методику управления инцидентами информационной безопасности;
- сущность аудита информационной безопасности;
- порядок организации аудита информационной безопасности;
- принципы управления логическим доступом к активам организации;
- принципы управления защищенной передачей данных;
- принципы управления безопасностью информационных систем.

уметь:

- разрабатывать частные политики информационной безопасности;
- оценивать информационные риски;
- разрабатывать предложения по совершенствованию системы управления информационной безопасностью;
- организовывать аудит информационной безопасности на основе действующих международных и отечественных стандартов по защите информации;

владеть:

- методами управления информационной безопасностью;
- методами оценки информационных рисков.

1.3. Предметом освоения дисциплины являются следующие объекты:

- управление информационной безопасностью;
- стандарты систем и процессов управления информационной безопасностью;
- политика информационной безопасности;
- методы управления информационной безопасностью;
- система управления информационной безопасностью;
- процессный подход;
- оценка рисков информационной безопасности;
- обработка рисков информационной безопасности;
- инциденты информационной безопасности;
- аудит информационной безопасности;
- метрики эффективности;
- управление логическим доступом к активам организации;
- управление защищенной передачей данных.

1.4. Место дисциплины в структуре профессиональной подготовки выпускников

Дисциплина «Управление информационной безопасностью» 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 подготовки (специальности).

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

Таблица 1.3. – Дисциплины, направленные на формирование компетенций

Код	Наименование компетенций	Предшествующие дисциплины	Последующие дисциплины
УПК-1	Способность принимать участие в эксплуатации подсистем управления информационной безопасностью предприятия, принимать организационно-управленческие решения в нестандартных ситуациях и нести за них ответственность	Организационное и правовое обеспечение информационной безопасностью	Комплексная защита информации на предприятии
УПК-2	Способность проводить анализ и оценку состояния защищенности объектов информатизации, участвовать в проектировании системы управления информационной безопасностью на основе действующих международных и отечественных стандартов по защите информации	Техническая защита информации	Организация и управление службой защиты информации на предприятии

2. Требования к результатам освоения учебной дисциплины

Дисциплина обеспечивает формирование компетенций УПК-1 и УПК-2:

2.1. Дисциплинарная карта компетенции УПК-1

Код УПК-1	**Формулировка унифицированной дисциплинарной компетенции** Способность принимать участие в эксплуатации подсистем управления информационной безопасностью предприятия, принимать организационно-управленческие решения в нестандартных ситуациях и нести за них ответственность

Требования к компонентному составу компетенции

Перечень компонентов	Виды учебной работы	Средства оценки
В результате освоения компетенции, студент знает: – цели и задачи управления информационной безопасностью; – принципы формирования политики информационной безопасности; – основные методы управления информационной безопасностью; – принципы управления логическим доступом к активам организации; – принципы управления защищенной передачей данных; – принципы управления безопасностью информационных систем;	Лекции Семинарские занятия Самостоятельная работа студентов по изучению теоретического материала Экзамен	Вопросы текущего, рубежного и итогового контроля
умеет: – разрабатывать частные политики информационной безопасности; – разрабатывать предложения по совершенствованию системы управления информационной безопасностью;	Практические занятия Самостоятельная работа студентов по решению практических задач	Отчет за выполнение практических заданий на ПЗ Отчёт по индивидуальным заданиям по модулю Темы ПЗ и ИЗМ
владеет: – методами управления информационной безопасностью.	Самостоятельная работа студентов по решению практических задач Самостоятельная работа по индивидуальному заданию	Отчет за выполнение практических заданий на ПЗ Отчёт по индивидуальным заданиям по модулю Темы ПЗ и ИЗМ

2.2. Дисциплинарная карта компетенции УПК-2

Код УПК-2	**Формулировка унифицированной дисциплинарной компетенции** Способность проводить анализ и оценку состояния защищенности объектов информатизации, участвовать в проектировании системы управления информационной безопасностью на основе действующих международных и отечественных стандартов по защите информации

Требования к компонентному составу компетенции

Перечень компонентов	Виды учебной работы	Средства оценки
В результате освоения компетенции, студент знает: – стандарты систем и процессов управления информационной безопасностью; – порядок оценки рисков информационной безопасности; – методы обработки рисков информационной безопасности; – методику управления инцидентами информационной безопасности; – сущность аудита информационной безопасности; – порядок организации аудита информационной безопасности;	Лекции Семинарские занятия Самостоятельная работа студентов по изучению теоретического материала Экзамен	Вопросы текущего, рубежного и итогового контроля
умеет: – оценивать информационные риски; – организовывать аудит информационной безопасности на основе действующих международных и отечественных стандартов по защите информации;	Практические занятия Самостоятельная работа студентов по решению практических задач	Отчет за выполнение практических заданий на ПЗ Отчёт по индивидуальным заданиям по модулю Темы ПЗ и ИЗМ
владеет: – методами оценки информационных рисков.	Самостоятельная работа студентов по решению практических задач Самостоятельная работа по индивидуальному заданию	Отчет за выполнение практических заданий на ПЗ Отчёт по индивидуальным заданиям по модулю Темы ПЗ и ИЗМ

3. Объем дисциплины и виды учебной работы

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

3.2. Основными видами аудиторной работы по дисциплине являются:

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

3.3. Основными видами самостоятельной работы по дисциплине являются:

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

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

Таблица 3.1 – Объём и виды учебной работы

№ п.п.	Виды учебной работы	Трудоёмкость, ч	Форма представления результатов
1	2	3	4
1	**Аудиторная работа**	**54**	
	- в том числе в интерактивной форме	14	
	- лекции (Л)	24	конспект лекций
	- в том числе в интерактивной форме	4	
	- практические занятия (ПЗ), семинарские занятия (СЗ)	28	отчёт о выполнении
	- в том числе в интерактивной форме	10	
	Контроль самостоятельной работы (КСР)	2	
2	**Самостоятельная работа студентов** (СРС)	**62**	
	- самостоятельное изучение теоретического материала (ИТМ)	32	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)**	 **152** **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		4	2	2		8
		2	4	2	2		4	2	2		8
		3	4	2	2		6	2	4		10
		4	6,5	2	4	0,5	6	4	2		12,5
	Всего по модулю:		**18,5**	8	10	0,5	**20**	10	10		**38,5**
2	2	5	4	2	2		4	2	2		8
		6	4	2	2		4	2	2		8
		7	4	2	2		4	2	2		8
		8	4	2	2		6	4	2		10
		9	4,5	2	2	0,5	6	4	2		10,5
	Всего по модулю:		**20,5**	10	10	0,5	**24**	14	10		**44,5**
3	3	10	4	2	2		4	2	2		8
		11	4	2	2		6	2	4		10
		12	7	2	4	1	8	4	4		15
	Всего по модулю:		**15**	6	8	1	**18**	8	10		**33**
	Итоговая аттестация										**36**
	Итого		**54**	**24**	**28**	**2**	**62**	**32**	**30**	**36**	**152/4**

4.2. Содержание разделов и тем учебной дисциплины

Модуль 1. Основы управления информационной безопасностью
Раздел 1. Основы управления информационной безопасностью
АРС: Л - 8 ч, ПЗ, СЗ - 10 ч., КСР – 0,5 ч., СРС: ИТМ - 10 ч., ИЗМ (ИЗМ-1) - 10 ч.

Тема 1.Введение в дисциплину «Управление информационной безопасностью». Цель и задачи изучения дисциплины. Базовая терминология. Система и системный подход. Процесс и процессный подход. Сущность и функции управления. Циклическая модель улучшения процессов. Понятие системы управления. Принципы управления. Цели и задачи управления информационной безопасностью.

Тема 2. Стандартизация систем и процессов управления информационной безопасностью. История развития стандартизации в области ИБ. Основные стандарты и методологии по управлению информационной безопасностью. Серия стандартов ISO 27000. Стандарты банковской системы Российской Федерации СТО БР ИББС. Рекомендации в области стандартизации. Стандарты на отдельные процессы управления информационной безопасностью и оценку безопасности информационных технологий: ISO\IEC 13335, ISO\IEC 15408, ISO\IEC 18045, BS 25999/25777, ГОСТ Р 53647. Стандарты CoBiT. Преимущества и недостатки применения основных стандартов в области информационной безопасности.

Тема 3. Политика информационной безопасности. Понятие политики информационной безопасности. Цели, требования и принципы при разработке и внедрении политики информационной безопасности. Порядок разработки частной политики информационной безопасности. Содержание и жизненный цикл политики информационной безопасности. Ответственность за исполнение политики информационной безопасности.

Тема 4. Управление и система управления информационной безопасностью. Деятельность по обеспечению информационной безопасностью организации. Основные методы управления информационной безопасностью. Управление информационной безопасностью информационно-телекоммуникационными технологиями организации. Система управления информационной безопасностью организации (СУИБ). Процессный подход в рамках управления информационной безопасностью организации. Работа с процессами СУИБ организацией. Стратегии построения и внедрения процессов СУИБ организацией. Совершенствование СУИБ.

Модуль 2. Управление рисками, инцидентами и аудит информационной безопасности
Раздел 3. Управление рисками, инцидентами и аудит информационной безопасности
АРС: Л - 10 ч, ПЗ, СЗ - 10 ч., КСР – 0,5 ч., СРС: ИТМ - 14 ч., ИЗМ (ИЗМ-1) - 10 ч.

Тема 5. Оценка рисков информационной безопасности. Нормативное обеспечение управления рисками информационной безопасности. Основы рисковой деятельности. Сущность и роль управления рисками информационной безопасности. Порядок оценки рисков информационной безопасности. Методы оценки рисков информационной безопасности.

Тема 6. Обработка рисков информационной безопасности. Процесс обработки рисков как этап управления рисками информационной безопасности. Варианты обработки рисков. Принятие, коммуникация, мониторинг и пересмотр рисков информационной безопасности. Обеспечение управления рисками информационной безопасности.

Тема 7. Управление инцидентами информационной безопасности. Нормативная база управления инцидентами информационной безопасности. Сущность процесса управления инцидентами информационной безопасности. Система управления инцидентами информационной безопасности. Этапы процесса управления инцидентами информационной безопасности.

Тема 8. Сущность аудита информационной безопасности. Назначение и цели аудита информационной безопасности. Виды аудита. Принципы проведения аудита информационной безопасности. Управление программой аудита информационной безопасности. Требования к аудитору информационной безопасности и оценка его работы. Измерение эффективности СУИБ. Метрики эффективности.

Тема 9. Содержание и организация аудита информационной безопасности. Этапы и организация работ по проведению аудита информационной безопасности. Области и критерии аудита информационной безопасности. Анализ документации. Интервьюирование персонала и непосредственное наблюдение за деятельностью. Подготовку и утверждение отчета по аудиту информационной безопасности. Разработка мероприятий и проработка решений по устранению выявленных нарушений.

Модуль 3. Технические аспекты управления информационной безопасностью
Раздел 3. Технические аспекты управления информационной безопасностью
АРС: Л - 6 ч, ПЗ, СЗ - 8 ч., КСР – 1 ч., СРС: ИТМ - 8 ч., ИЗМ (ИЗМ-1) - 10 ч.

Тема 10. Управление логическим доступом к активам организации. Политика в отношении логического доступа. Управление доступом пользователей. Обязанности пользователя при доступе к активам. Управление сетевым доступом. Управление доступом к операционной системе. Управление доступом к приложениям. Работа с мобильными устройствами в дистанционном режиме.

Тема 11. Управление защищенной передачей данных и операционной деятельностью. Документированные процедуры. Разделение полномочий. Разграничение сред разработки и промышленной эксплуатации. Доступ к средствам обработки информации сторонних лиц и/или организаций. Планирование нагрузки и приемка систем. Защита от вредоносного программного обеспечения. Управление сетевыми ресурсами. Защита носителей информации. Обмен информацией и программного обеспечения. Вспомогательные операции.

Тема 12. Разработка и обслуживание информационных систем. Выработка требований по обеспечению информационной безопасности систем. Информационная безопасность приложений, исходных текстов программного обеспечения, исполняемых и системных файлов. Информационная безопасность данных и учетных записей. Информационная безопасность в процессах разработки и сопровождения информационных систем. Защитные меры, связанные с использованием криптографии. Управление конфигурациями, изменениями и обновлениями.

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	Сущность и функции управления информационной безопасностью (СЗ)
2	2	Основные стандарты по управлению информационной безопасностью (СЗ)
3	3	Разработка политика информационной безопасности (ПЗ)
4	4	Система управления информационной безопасностью (СЗ)
5	4	Построение и внедрение процессов СУИБ организацией (ПЗ)
6	5	Оценка рисков информационной безопасности (ПЗ)
7	6	Обработка рисков информационной безопасности (ПЗ)
8	7	Управление инцидентами информационной безопасности (ПЗ)
9	8	Назначение, цели и виды аудита информационной безопасности (СЗ)
10	9	Организация и проведение аудита информационной безопасностью (ПЗ)
11	10	Управление логическим доступом к активам организации (ПЗ)
12	11	Управление защищенной передачей данных и операционной деятельностью (ПЗ)
13	12	Разработка и обслуживание информационных систем (ПЗ)
14	12	Управление конфигурациями, изменениями и обновлениями (ПЗ)

4.4 Перечень тем лабораторных работ

Не предусмотрены.

4.5 Виды самостоятельной работы студентов

Таблица 4.5 – Виды самостоятельной работы студентов (СРС)

Номер темы (раздела) дисциплины	Вид самостоятельной работы студентов	Трудоёмкость, часов
1	2	3
1	ИТМ: Базовая терминология в области управления информационной безопасностью	2

1	2	3
2	ИТМ: Рекомендации в области стандартизации банковской системы Российской Федерации РС БР ИББС	2
3	ИТМ: Ответственность за исполнение политики информационной безопасности	2
4	ИТМ: Управление информационной безопасностью информационно-телекоммуникационными технологиями организации	4
4	ИЗМ: В соответствии с заданием для модуля 1, п.п. 4.5.1	10
5	ИТМ: Нормативное обеспечение управления рисками информационной безопасности	2
6	ИТМ: Обеспечение управления рисками информационной безопасности	2
7	ИТМ: Нормативная база управления инцидентами информационной безопасности	2
8	ИТМ: Требования к аудитору информационной безопасности и оценка его работы	2
9	ИТМ: Разработка мероприятий и проработка решений по устранению выявленных нарушений	2
9	ИЗМ: В соответствии с заданием для модуля 2, п.п. 4.5.1	10
10	ИТМ: Работа с мобильными устройствами в дистанционном режиме	2
11	ИТМ: Защита носителей информации	4
12	ИТМ: Управление конфигурациями, изменениями и обновлениями	4
12	ИЗМ: В соответствии с заданием для модуля 3, п.п. 4.5.1	10
	Итого: в **ч** / в **ЗЕ**	**62/1,7**

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

Индивидуальное задание представляет собой комплекс задач по формированию политики информационной безопасности предприятия (организации), а также частных политик информационной безопасности по отдельным направлениям, в соответствии с вариантом. Особенности бизнес-процессов предприятия (организации), необходимых для формирования политики информационной безопасности определяются вариантом индивидуальных заданий по дисциплинам «Разработка и эксплуатация защищенных автоматизированных систем», «Комплексная защита информации на предприятии».

Последовательность разработки политики информационной безопасности (организации) осуществляется поэтапно, в соответствии с последовательностью изучаемых разделов учебной дисциплины, в соответствии с требованиями стандартов по управлению информационной безопасностью.

Раздел 1, модуль 1

Тема 1. Цели и задачи управления информационной безопасностью предприятия.
Тема 2. Стандарты по управлению информационной безопасностью как основа политики информационной безопасности предприятия.
Тема 3. Содержание и жизненный цикл политики информационной безопасности.
Тема 4. Система управления информационной безопасностью предприятия.

Раздел 2, модуль 2

Тема 5. Порядок оценки рисков информационной безопасности предприятия.
Тема 6. Порядок обработки рисков информационной безопасности предприятия.
Тема 7. Порядок управления инцидентами информационной безопасности предприятия.
Тема 8. Порядок оценки эффективности системы управления информационной безопасностью предприятия.
Тема 9. Этапы и организация работ по проведению аудита информационной безопасности предприятия.

Раздел 3, модуль 3

Тема 10. Частная политика в отношении логического доступа к активам предприятия.
Тема 11. Частная политика по управлению защищенной передачей данных и операционной деятельностью.
Тема 12. Частная политика по разработке и сопровождению информационных систем.

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, на основе действующих международных и отечественных стандартов по управлению информационной безопасностью.

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 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 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:					
– цели и задачи управления информационной безопасностью;	+	+	+		+
– стандарты систем и процессов управления информационной безопасностью;	+	+	+		+
– принципы формирования политики информационной безопасности;	+	+	+		+
– основные методы управления информационной безопасностью;	+	+	+		+
– порядок оценки рисков информационной безопасности;	+	+	+		+
– методы обработки рисков информационной безопасности;	+	+	+		+
– методику управления инцидентами информационной безопасности;	+	+	+		+
– сущность аудита информационной безопасности;	+	+	+		+
– порядок организации аудита информационной безопасности;	+	+	+		+
– принципы управления логическим доступом к активам организации;	+	+	+		+
– принципы управления защищенной передачей данных;	+	+	+		+
– принципы управления безопасностью информационных систем.	+	+	+		+
Умеет:					
– разрабатывать частные политики информационной безопасности;			+	+	
– оценивать информационные риски;			+	+	
– разрабатывать предложения по совершенствованию системы управления информационной безопасностью;			+	+	
– организовывать аудит информационной безопасности на основе действующих международных и отечественных стандартов по защите информации;			+	+	
Владеет:					
– методами управления информационной безопасностью;			+	+	
– методами оценки информационных рисков.			+	+	

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		**24**
Практические, семинарские занятия (ПЗ, СЗ)		2		2	2		2	2	2		2	2	2	2	2	2	2	2	**28**
Самост. изучение теоретического материала		2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2		**32**
Вып. инд. заданий (ИЗМ)		2	2	2	2	2		2	2	2	2	2		2	2	2	2	2	**30**
КСР						0,5							0,5					1	**2**
Модуль:	**1**						**2**												
Контр. тестирование						+							+					+	
Дисциплин. контроль																			**Экз.**

8. Учебно-методическое и информационное обеспечение дисциплины

8.1. Карта обеспеченности дисциплины учебно-методической литературой

Управление информационной безопасностью	*Профессиональный цикл*	
полное название дисциплины	[x] обязат. / [ ] по выбору студента	[x] базовая часть цикла / [ ] вариативная часть цикла

090900.62 090303.65	**«Информационная безопасность»**, профиль «Комплексная защита объектов информатизации» **«Информационная безопасность автоматизированных систем»**, специализация «Обеспечение информационной безопасности распределенных информационных систем»
код направления / специальности	*полное название направления/ специальности*

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

2015 семестр(ы) 7 количество групп 2
количество студентов 40

Шабуров Андрей Сергеевич, доцент,
электротехнический факультет,
кафедра АТ, телефон: 239-18-16.

СПИСОК ИЗДАНИЙ

№	Библиографическое описание	Количество экземпляров в библиотеке
1	2	3
	1. Основная литература	
1	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	Милославская Н.Г. Управление рисками информационной безопасности : учебное пособие для вузов / Н. Г. Милославская, М. Ю. Сенаторов, А. И. Толстой .— 2-е изд., испр.— Москва : Горячая линия-Телеком, 2014 .— 130 с.	15
3	Милославская Н.Г. Управление инцидентами информационной безопасности и непрерывностью бизнеса : учебное пособие для вузов / Н. Г. Милославская, М. Ю. Сенаторов, А. И. Толстой .— 2-е изд., испр.— Москва : Горячая линия-Телеком, 2014 .— 168 с.	5
4	Милославская Н.Г. Технические, организационные и кадровые аспекты управления информационной безопасностью : учебное пособие для вузов / Н. Г. Милославская, М. Ю. Сенаторов, А. И. Толстой .— Москва : Горячая линия-Телеком, 2012 .— 214 с.	5
	2. Дополнительная литература	
	2.1. Учебные и научные издания	
1	Анисимов А.А. Менеджмент в сфере информационной безопасности: учебное пособие / А. А. Анисимов ; Интернет-университет информационных технологий.— Москва : ИНТУИТ : БИНОМ. Лаб. знаний, 2010. - 175 с.	2
2	Грачева М.В. Управление рисками в инновационной деятельности: учебное пособие для вузов / М. В. Грачева, С.В. Ляпина. - Москва: ЮНИТИ, 2010 - 351 с.	8
3	Петренко С. А. Политики информационной безопасности / С.А. Петренко, В.А. Курбатов .— М. : Академия АйТи, 2006 .— 394 с .	2

Основные данные об обеспеченности на _____
(дата составления рабочей программы)

Основная литература [x] обеспечена [ ] не обеспечена

Дополнительная литература [x] обеспечена [ ] не обеспечена

Зав. отделом комплектования научной библиотеки _____ Н. В. Тюрикова

Текущие данные об обеспеченности на _____
(дата контроля литературы)

Основная литература [ ] обеспечена [ ] не обеспечена

Дополнительная литература [ ] обеспечена [ ] не обеспечена

Зав. отделом комплектования научной библиотеки _____ Н.В. Тюрикова

Карта книго-обеспеченности в библиотеку сдана

8.2 Компьютерные обучающие и контролирующие программы

Таблица 8.1 – Используемые компьютерные обучающие программы

№ п/п	Вид учебного занятия	Наименование программного продукта	Рег. номер	Назначение
1	2	3	4	5
1	ПЗ, СЗ	Базы данных правовой информации – Гарант - www. garant.ru; – Информационно-справочная система «Консультант Плюс».	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 кафедры. Подпись заведующего кафедрой
1.	Содержание стр. 1, кроме абзацев 6-9, изложить в редакции, приведенной на стр. 1а.	Протокол заседания кафедры АТ от «16 » января 2017 г. № 18 Зав. кафедрой АТ д-р техн. наук, проф. _____ А.А. Южаков
	Содержание стр. 2 (абзацы 1-7) изложить в редакции, приведенной на стр. 2а.	
	Изменения шифров и формулировок компетенций (стр. 3 - 5, 6-8,) внесены на основании перехода на ФГОС ВО: по 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.: - общепрофессиональную компетенцию ОК-6 считать профессиональной компетенцией ПК-11 с формулировкой «Способность разрабатывать политику информационной безопасности автоматизированной системы»; - изменить шифр дисциплинарной компетенции с ОК-6.С3.Б7 на ПК-11.Б1.Б28; - профессиональную компетенцию ПК-18 считать профессиональной компетенции ПК-12 с формулировкой «Способность участвовать в проектировании системы управления информационной безопасностью автоматизированной системы»; - изменить шифр дисциплинарной компетенции с ПК-18.С3.Б7 на ПК-12.Б1.Б28.	
	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 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 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.		