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
д-р техн. наук
_____ Н. В. Лобов
«__» _____ 2015 г.

УЧЕБНО-МЕТОДИЧЕСКИЙ КОМПЛЕКС ДИСЦИПЛИНЫ
«Безопасность сетей ЭВМ»

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 (степень) подготовки: специалист

Выпускающая кафедра: «Автоматика и телемеханика»

Форма обучения: Очная

Курс: 4,5 **Семестр(ы):** 8,9

Трудоёмкость:
Кредитов по рабочему учебному плану: 10 ЗЕ
Часов по рабочему учебному плану: 360 ч

Виды контроля:
Экзамен: **- 8,9 сем** Зачёт: Курсовой проект: **-** Курсовая работа: **8 сем**

Пермь
2015

Рабочая программа дисциплины Безопасность сетей ЭВМ
разработана на основании:

- федерального государственного образовательного стандарта высшего профессионального образования, утверждённого приказом Министерства образования и науки Российской Федерации «17» января 2011 г. номер приказа «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 09030307.65 «Обеспечение информационной безопасности распределенных информационных систем, утверждённой «24» июня 2013 г.;
- базового учебного плана очной формы обучения по специальности 090303.65 «Информационная безопасность автоматизированных систем», специализации 09030307.65 «Обеспечение информационной безопасности распределенных информационных систем», утверждённого «29» августа 2011 г.

Рабочая программа согласована с рабочими программами дисциплин Основы информационной безопасности, Криптографические методы защиты информации, Организационное и правовое обеспечение информационной безопасности, Техническая защита информации 1 (Технические средства охраны), Техническая защита информации 2, Управление информационной безопасностью, Вычислительная техника и информационные технологии, Основы построения инфокоммуникационных систем и сетей, Программно-аппаратные средства защиты информации, Разработка и эксплуатация защищенных автоматизированных систем.

Разработчик
канд. техн. наук, доцент _____ И.И. Безукладников

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

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 _____ А.А. Южаков

Рабочая программа одобрена методической комиссией электротехнического факультета «18» 06 2015 г., протокол № 37.

Председатель методической комиссии
электротехнического факультета
канд. техн. наук, профессор _____ А.Л. Гольдштейн

Согласовано

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

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

1 Общие положения

1.1 Цель дисциплины – формирование у студентов компетентности в области информационной безопасности инфокоммуникационных сетей ЭВМ.

В процессе изучения данной дисциплины студент осваивает части следующих компетенций:

- способность к освоению новых образцов программных, технических средств и информационных технологий (ПК-8)
- способность участвовать в разработке компонентов автоматизированных систем в сфере профессиональной деятельности (ПК-19).
- способность разрабатывать модели угроз и модели нарушителя информационной безопасности в распределенных информационных системах (ПСК-07.02.2014)

1.2 Задачи дисциплины:

- **Изучение** базовой инфраструктуры инфокоммуникационных сетей, основных устройств и систем, требований к обеспечению информационной безопасности, соответствующих стандартов, технических спецификаций, протоколов и технологий;
- Формирование **умений** по созданию, настройке и эксплуатации безопасных сетей ЭВМ
- **Овладение** навыками по использованию компонентов защищенных сетей ЭВМ, способностью разрабатывать модели угроз и модели нарушителей ИБ на основе исходных данных о сети

1.3 Предметом освоения дисциплины являются следующие объекты:

- Принципы построения защищенных компьютерных телекоммуникационных сетей (ЗКТС, сетей ЭВМ)
- Методы и проблемы оценивания угроз безопасности, угрозы безопасности, стандарты информационной безопасности
- Классификация типовых угроз информационной безопасности для ЗКТС (вирусные угрозы, трояны, сетевые черви, спам, и т.д.)
- Требования к архитектуре информационных систем и их компонентам для обеспечения безопасности функционирования;
- Модели и теоремы безопасности на основе дискреционной политики, модели и теоремы безопасности на основе мандатной политики,
- Скрытые каналы утечки информации, модели и механизмы обеспечения целостности данных
- Нормативные документы по метрологии, стандартизации и сертификации программных и аппаратных средств защиты.
- Типовые аппаратные и программные средства обеспечения информационной безопасности

1.4 Место дисциплины в структуре профессиональной подготовки выпускников.

Дисциплина «Безопасность сетей ЭВМ» относится к базовой части цикла профессиональных дисциплин и является обязательной при освоении ООП подготовки специалистов по специализации 09030307.65 «Обеспечение информационной безопасности распределенных информационных систем».

После изучения дисциплины обучающийся должен освоить части указанных в пункте 1.1 компетенций и демонстрировать следующие результаты:

- **знать:**
  - основные направления развития информационно-коммуникационных технологий объекта защиты,
  - методы оценки эффективности функционирования систем информационной безопасности, способы оценки затрат и рисков;
  - типовые структуры, принципы организации, средства и технологии обеспечения информационной безопасности объектов защиты
  - современные методы обеспечения информационной безопасности, вновь вводимые отечественные и международные стандарты;
  - основные угрозы информационной безопасности объектов и методы противодействия им;
  - требования к архитектуре информационных систем и их компонентам для обеспечения безопасности функционирования;
  - нормативные документы по метрологии, стандартизации и сертификации программных и аппаратных средств защиты.
  - структуры и организацию построения узлов ЗКТС;
  - методы обеспечения надежности ЗКТС;

- **уметь:**
  - анализировать направления развития информационно-коммуникационных технологий объекта защиты, прогнозировать эффективность функционирования систем информационной безопасности;
  - обосновывать выбор структуры, принципов организации, комплекса средств и технологий обеспечения информационной безопасности объектов защиты;
  - осваивать и адаптировать к защищаемым объектам современные методы обеспечения информационной безопасности, вновь вводимые отечественные и международные стандарты;
  - анализировать угрозы информационной безопасности объектов и разрабатывать методы противодействия им;
  - использовать методы и средства определения технологической безопасности функционирования распределенной информационной системы;
  - применять нормативные документы по метрологии, стандартизации и сертификации на практике.

- **владеть:**
  - навыками организации комплекса средств и технологий обеспечения информационной безопасности объектов защиты;
  - навыками применения современных методов обеспечения информационной безопасности, внедрения на объекты защиты вновь вводимых и существующих отечественных и международных стандартов
  - навыками анализа угроз информационной безопасности объектов и разработки соответствующих методов противодействия им

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-8	Способность к освоению новых образцов программных, технических средств и информационных технологий	- Техническая защита информации 1 (Технические средства охраны) - Управление информационной безопасностью - Электроника и схемотехника 3 (Электропитание устройств и систем) - Разработка и эксплуатация защищенных автоматизированных систем - Информатика 2 (Языки программирования) - Теория электрических цепей	-
ПК-19	Способность участвовать в разработке компонентов автоматизированных систем в сфере профессиональной деятельности	- Управление информационной безопасностью - Электроника и схемотехника 3 (Электропитание устройств и систем) - Инженерная и компьютерная графика - Разработка и эксплуатация защищенных автоматизированных систем	-
ПСК-07.02.2014	Способность разрабатывать модели угроз и модели нарушителя информационной безопасности в распределенных информационных системах	- Разработка и эксплуатация защищенных автоматизированных систем	-

2 Требования к результатам освоения учебной дисциплины

Учебная дисциплина обеспечивает формирование части компетенций ПК-8, ПК-19 и ПСК-07.02.2014.

2.1 Дисциплинарная карта компетенции ПК-8

Код	Формулировка компетенции
ПК-8	Способность к освоению новых образцов программных, технических средств и информационных технологий

Код	Формулировка дисциплинарной части компетенции
ПК-8.С3.Б.17	Способность к освоению новых образцов программных, технических средств и информационных технологий при создании защищенных компьютерных телекоммуникационных сетей (сетей ЭВМ)

Требования к компонентному составу части компетенции

Перечень компонентов	Виды учебной работы	Средства оценки
В результате освоения дисциплинарной части компетенции студент **Знает:** - основные направления развития информационно-коммуникационных технологий объекта защиты, (ПК-8.С3.Б.17-1з) - методы оценки эффективности функционирования систем информационной безопасности, способы оценки затрат и рисков; (ПК-8.С3.Б.17-2з) - типовые структуры, принципы организации, средства и технологии обеспечения информационной безопасности объектов защиты (ПК-8.С3.Б.17-3з)	Лекции. Самостоятельная работа студентов по изучению теоретического материала. Написание рефератов.	Тестовые вопросы текущего и рубежного контроля. Темы рефератов. Вопросы, задаваемые на защите рефератов
Умеет: - анализировать направления развития информационно-коммуникационных технологий объекта защиты, прогнозировать эффективность функционирования систем информационной безопасности; (ПК-8.С3.Б.17-1у) - обосновывать выбор структуры, принципов организации, комплекса средств и технологий обеспечения информационной безопасности объектов защиты; (ПК-8.С3.Б.17-2у)	Практические занятия. Лабораторные работы. Самостоятельная работа студентов по решению индивидуальных заданий по теме практических (ИЗПЗ) и лабораторных работ (ИЗЛР).	Тестовые вопросы текущего и рубежного контроля. Индивидуальные задания по теме практических и лабораторных работ. Вопросы, задаваемые на защите отчетов по ИЗПЗ и ИЗЛР

Владеет: - навыками организации комплекса средств и технологий обеспечения информационной безопасности объектов защиты; (ПК-8.С3.Б.17-1в)	Самостоятельная работа по подготовке к зачету. Выполнение индивидуального комплексного задания по дисциплине (ИКЗД).	Вопросы и практические задания на зачете. Задание на ИКЗД. Вопросы на защите отчета по ИКЗД.

2.2 Дисциплинарная карта компетенции ПК-19

Код	Формулировка компетенции
ПК-19	Способность участвовать в разработке компонентов автоматизированных систем в сфере профессиональной деятельности

Код	Формулировка дисциплинарной части компетенции
ПК-19.С3.Б.17	Способность участвовать в разработке компонентов автоматизированных систем в рамках создания защищенных компьютерных телекоммуникационных сетей (сетей ЭВМ)

Требования к компонентному составу части компетенции

Перечень компонентов	Виды учебной работы	Средства оценки
В результате освоения дисциплинарной части компетенции студент **Знает:** - современные методы обеспечения информационной безопасности, вновь вводимые отечественные и международные стандарты; (ПК-19.С3.Б.17-1з) - основные угрозы информационной безопасности объектов и методы противодействия им; (ПК-19.С3.Б.17-2з) - требования к архитектуре информационных систем и их компонентам для обеспечения безопасности функционирования; (ПК-19.С3.Б.17-3з)	Лекции. Самостоятельная работа студентов по изучению теоретического материала. Написание рефератов.	Тестовые вопросы текущего и рубежного контроля. Темы рефератов. Вопросы, задаваемые на защите рефератов
Умеет: - осваивать и адаптировать к защищаемым объектам современные методы обеспечения информационной безопасности, вновь вводимые отечественные и международные стандарты; (ПК-19.С3.Б.17-1у) - анализировать угрозы информационной безопасности объектов и разрабатывать методы противодействия им; (ПК-19.С3.Б.17-2у)	Практические занятия. Лабораторные работы. Самостоятельная работа студентов по решению индивидуальных заданий по теме практических (ИЗПЗ) и лабораторных работ (ИЗЛР).	Тестовые вопросы текущего и рубежного контроля. Индивидуальные задания по теме практических и лабораторных работ. Вопросы, задаваемые на защите отчетов по ИЗПЗ и ИЗЛР

Владеет: - навыками применения современных методов обеспечения информационной безопасности, внедрения на объекты защиты вновь вводимых и существующих отечественных и международных стандартов (ПК-19.С3.Б.17-1в)	Самостоятельная работа по подготовке к экзамену. Выполнение индивидуального комплексного задания по дисциплине (ИКЗД).	Вопросы и практические задания на экзамене. Задание на ИКЗД. Вопросы на защите отчета по ИКЗД.

2.3 Дисциплинарная карта компетенции ПСК-07.02.2014

Код	Формулировка компетенции
ПСК-07.02.2014	Способность разрабатывать модели угроз и модели нарушителя информационной безопасности в распределенных информационных системах

Код	Формулировка дисциплинарной части компетенции
ПСК-07.02.2014.С3.Б.17	Способность разрабатывать модели угроз и модели нарушителя информационной безопасности в защищенных компьютерных телекоммуникационных сетях (сетях ЭВМ)

Требования к компонентному составу части компетенции

Перечень компонентов	Виды учебной работы	Средства оценки
В результате освоения дисциплинарной части компетенции студент **Знает:** - нормативные документы по метрологии, стандартизации и сертификации программных и аппаратных средств защиты. (ПСК-07.02.2014.С3.Б.17-1з) - структуры и организацию построения узлов ЗКТС; (ПСК-07.02.2014.С3.Б.17-2з) - методы обеспечения надежности ЗКТС; (ПСК-07.02.2014.С3.Б.17-3з)	Лекции. Самостоятельная работа студентов по изучению теоретического материала. Написание рефератов.	Тестовые вопросы текущего и рубежного контроля. Темы рефератов. Вопросы, задаваемые на защите рефератов
Умеет: - использовать методы и средства определения технологической безопасности функционирования распределенной информационной системы; (ПСК-07.02.2014.С3.Б.17-1у)	Практические занятия. Лабораторные работы. Самостоятельная работа студентов по решению индивидуальных заданий по теме практических	Тестовые вопросы текущего и рубежного контроля. Индивидуальные задания по теме практических и лабораторных работ. Вопросы, задаваемые на защите отчетов по ИЗПЗ и ИЗЛР

- применять нормативные документы по метрологии, стандартизации и сертификации на практике. (ПСК-07.02.2014.С3.Б.17-2у)	(ИЗПЗ) и лабораторных работ (ИЗЛР).	
Владеет: - навыками анализа угроз информационной безопасности объектов и разработки соответствующих методов противодействия им (ПСК-07.02.2014.С3.Б.17-1в)	Самостоятельная работа по подготовке к экзамену. Выполнение индивидуального комплексного задания по дисциплине (ИКЗД).	Вопросы и практические задания на экзамене. Задание на ИКЗД. Вопросы на защите отчета по ИКЗД.

3 Структура учебной дисциплины по видам и формам учебной работы

Таблица 3.1 – Объём и виды учебной работы

№ п.п.	Виды учебной работы	Трудоёмкость		
		по семестрам		всего
		8	9	
1	2	3	4	4
1	**Аудиторная работа / в том числе в интерактивной форме**	**45/45**	**90/74**	**135/119**
	Лекции (Л) / в том числе в интерактивной форме	16/16	32/16	48/32
	Практические занятия (ПЗ) / в том числе в интерактивной форме	-	18/18	18/18
	Лабораторные работы (ЛР)	27/27	36/36	63/63
2	**Контроль самостоятельной работы (КСР)**	**2**	**4**	**6**
3	**Самостоятельная работа студентов (СРС)**	**63**	**90**	**153**
	Изучение теоретического материала (ИТМ)	20	20	40
	Выполнение индивидуальных заданий по тематике практических занятий (ИЗПЗ)	-	16	16
	Выполнение индивидуальных заданий по тематике лабораторных работ (ИЗЛР)	16	16	16
	Курсовая работа (КР)	27	-	27
	Индивидуальной комплексное задание по дисциплине (ИКЗД)	-	38	38
4	**Итоговая аттестация по дисциплине**	**экзамен 36**	**экзамен 36**	**72**
5	**Трудоёмкость дисциплины** **Всего:** **в часах (ч)** **в зачётных единицах (ЗЕ)**	 **144** **4**	 **216** **6**	 **360** **10**

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)							Трудоёмкость, ч / ЗЕ
			аудиторная работа				КСР	аттестация	самостоятельная работа	
			всего	Л	ПЗ	ЛР				
1	2	3	4	5	6	7	8	9	10	11
1	1	Введение	2	2						2
		1	9	4		5			ИТМ-5 ИЗЛР-4 КР-6	24
		2	9	2		6	1		ИТМ-5 ИЗЛР-4 КР-7	25
	Всего по модулю:		**20**	**8**		**11**	**1**		**31**	**51/1,5**
2	2	3	12	4		8			ИТМ-5 ИЗЛР-4 КР-7	28
		4	13	4		8	1		ИТМ-5 ИЗЛР-4 КР-7	29
	Всего по модулю:		**25**	**8**		**16**	**1**		**32**	**57/1,5**
Итоговая аттестация:								**36**		**36/1**
Всего за 8 семестр:			**45**	**16**	**-**	**27**	**2**	**36**	**63**	**144/4**
3	3	5	23	8	4	10	1		ИТМ-5 ИЗЛР-4 ИЗПЗ-4 ИКЗД-10	46
		6	21	8	4	8	1		ИТМ-5 ИЗПЗ-4 ИЗЛР-4 ИКЗД-9	43
	Всего по модулю:		**44**	**16**	**8**	**18**	**2**		**45**	**89/2,5**
4	4	7	23	8	4	10	1		ИТМ-5 ИЗПЗ-4 ИЗЛР-4 ИКЗД-10	46
		8	21	6	6	8	1		ИТМ-5 ИЗПЗ-4 ИЗЛР-4 ИКЗД-9	43
		Заключение	2	2						2
	Всего по модулю:		**46**	**16**	**10**	**18**	**2**		**45**	**90/2,5**
Итоговая аттестация:								**36**		**36/2**
Всего за 9 семестр:			**90**	**32**	**18**	**36**	**4**	**36**	**90**	**216/6**
Итого:			**135**	**48**	**18**	**63**	**6**	**72**	**153**	**360/10**

4.2 Содержание разделов и тем учебной дисциплины

Модуль 1 (Раздел 1). Принципы построения узлов защищенных компьютерных и телекоммуникационных сетей

Л – 8 ч, ЛР – 11 ч, СРС – 31 ч, КСР – 1 ч.

Введение

Основные понятия, термины и определения. Предмет и задачи дисциплины.

Тема 1. Защищенные компьютерные и телекоммуникационные сети

Структура узлов ЗТКС. Основные принципы построения узлов связи как стационарных, так и полевых. Оперативно-технические службы узлов связи и их взаимодействие. Обеспечение и поставка техники на узлы связи. Хранение техники на узлах связи. Возможные каналы утечки информации при эксплуатации узлов ЗТКС. Основные каналы утечки информации. Методы технической защиты абонентских и соединительных линий на узлах связи. Методы защиты информации на элементах узлов связи ЗТКС

Тема 2. Основные понятия о надежности систем ЗКТС

Основы теории надежности систем связи. Факторы, влияющие на надежность защищенных телекоммуникационных систем; модели надежности; оценка показателей надежности; методы обеспечения надежности; влияние человеческого фактора на надежность защищенных телекоммуникационных систем; испытания систем на надежность

Модуль 2 (Раздел 2). Политика и модели безопасности в защищенных компьютерных телекоммуникационных сетях.

Л – 8 ч, ЛР – 16 ч, СРС – 32 ч, КСР – 1 ч.

Тема 3. Угрозы безопасности в компьютерных системах

Понятие угрозы. Угрозы безопасности информации в компьютерных системах. Понятия "идентификация", "аутентификация", "авторизация", "спецификация", "классификация", "категорирование" и "каталогизация". Классификационные схемы (каталогизация) угроз. Теоретические (формальные) основы классификации — критерии выделения и таксономия классов (алгебраическая полнота в операциях пересечения и объединения классов). Примеры и проблемы теоретического обоснования каталогов угроз по зарубежным, отечественным и международным стандартам.

Тема 4. Политика и модели безопасности в компьютерных системах

Понятие политики безопасности. Модель безопасности как формализованное выражение политики безопасности. Модель безопасности как основа архитектурных, схемотехнических и программно-алгоритмических решений при создании защищенных КС, анализа систем защиты информации в КС. Со-

ставляющие модели безопасности — модель (формализация) компьютерной системы в аспекте безопасности информации, критерии, формализованные правила, алгоритмы, механизмы безопасного функционирования КС. Класс моделей конечных состояний.

Модуль 3 (Раздел 3). Детализированные модели информационной безопасности

Л – 16 ч, ПЗ – 8, ЛР – 18 ч, СРС – 45 ч, КСР – 2 ч.

Тема 5. Модели безопасности на основе дискреционной и мандатной политик

Общая характеристика политики дискреционного доступа. Тройки доступа: субъект-операция-объект. Модели дискреционного (избирательного) разграничения доступа и модели распространения прав доступа. Пятимерное пространство Хартсона как пример выражения дискреционного разграничения доступа на языке реляционной алгебры. Модели разграничения доступа на основе матрицы доступа. Принудительный и добровольный принцип управления доступом. Администраторы системы и владельцы объектов. Привилегии и предоставление (распространение) прав доступа. Общая характеристика политики мандатного (полномочного) доступа. Парадигма градуированного доверия пользователям (субъектам доступа) и градуированной степени конфиденциальности данных (объектов доступа). Уровни безопасности субъектов и объектов доступа. Правила безопасного мандатного доступа — запрет чтения вверх (NRU) и запрет записи вниз (NWD). Рефрексивность, антисимметричность и транзитивность отношений доступа. Функция уровня безопасности субъектов и объектов доступа.

Тема 6. Модели безопасности на основе тематической и ролевой политик

Общая характеристика политики тематического доступа. Тематическое классификационное множество и ее разновидности. Способы тематической классификации субъектов и объектов доступа на основе дескрипторных, иерархических и фасетных классификационных множеств. Критерии безопасности информационных потоков в системах тематического разграничения доступа. Общая характеристика политики ролевого (типизованного) доступа. Роль как типовой субъект доступа (функционально обособленное агрегирование прав доступа и полномочий выполнения процедур над данными). Две фазы организации ролевого доступа — создание ролей как типовых субъектов доступа с наделением их правами (полномочиями) доступа на основе дискреционной, мандатной, тематической или иной политики безопасности и назначение ролей пользователям.

Модуль 4 (Раздел 4). Базовые элементы и устройства обеспечения сетевой безопасности информационных систем

Л – 16 ч, ПЗ – 10, ЛР – 18 ч, СРС – 45 ч, КСР – 2 ч.

Тема 7. Межсетевые экраны, пакетная фильтрация и обнаружение атак

Классификация firewall'ов. Установление TCP-соединения. Пакетные фильтры. Пограничные роутеры. Пример набора правил пакетного фильтра. Stateful Inspection firewall'ы. Host-based firewall'ы. Персональные firewall'ы и персональные устройства firewall'а. Основные характеристики пакетных фильтров в ОС FreeBSD. ПО пакетных фильтров. OpenBSD Packet Filter (PF) и ALTQ. Указание необходимости использования PF. Опции ядра. Опции rc.conf. Указание необходимости использования ALTQ. Создание правил фильтрации. IPFILTER (IPF) firewall. Понятие системы обнаружения атак. Почему следует использовать IDS. Типы IDS. Базовая архитектура IDS. Совместное расположение Host и Target. Разделение Host и Target. Способы управления IDS. Централизованное управление. Частично распределенное управление. Полностью распределенное управление. Скорость реакции. Информационные источники. Network-Based IDS. Host-Based IDS. Application-Based IDS.

Тема 8. Технологии обеспечения комплексной безопасности сетевых инфраструктур

Топология сети. Демилитаризованная зона. Хостинг во внешней организации. Сетевые элементы. Роутер и firewall. Системы обнаружения проникновения (IDS). Сетевые коммутаторы и концентраторы. Список действий для обеспечения безопасности сетевой инфраструктуры. Администрирование web-сервера. Создание логов. Основные возможности создания логов. Дополнительные требования для создания логов. Возможные параметры логов. Просмотр и хранение лог-файлов. Автоматизированные инструментальные средства анализа лог-файлов. Процедуры создания backup web-сервера. Требования к аутентификации и шифрованию. Аутентификация, основанная на IP-адресе. Basic-аутентификация. Digest-аутентификация. SSL/TLS. Возможности SSL/TLS. Слабые места SSL/TLS. Пример SSL/TLS-сессии. Схемы шифрования SSL/TLS. Требования к реализации SSL/TLS. Список действий для технологий аутентификации и шифрования.

Заключение

4.3 Перечень тем практических занятий

Таблица 4.3 – Темы практических занятий

№ п.п.	Номер темы дисциплины	Наименование темы практического занятия
1	2	3
1	5	Модель безопасности как основа архитектурных, схемотехнических и программно-алгоритмических решений при создании защищенных КС, анализа систем защиты информации в КС. (ПЗ1, 4 ч)
2	5	Тематические решетки на основе классификационных множеств. (ПЗ2, 4 ч)
3	5,6	Сеансовая авторизация пользователя с одной или группой назначенных ему в системе ролей и доступ к объектам системы в соответствующей (соответствующих) роли (ролях) (ПЗ3, 4 ч)
4	5,7	Порядковое (ранговое) шкалирование компьютерных систем в аспекте безопасности на основе группирования (классификации) в пространстве шкалирования первичных факторов оценки (ПЗ4, 6 ч)

4.4 Перечень тем лабораторных работ

Таблица 4.4 – Темы лабораторных работ

№ п.п.	Номер темы дисциплины	Наименование темы лабораторной работы
1	2	3
1	1	Исследование каналов утечки информации в ЗКТС на примере полевой шины LonWorks и универсальной технологии Ethernet (ЛР1, 5 ч).
2	1,2	Анализ типовых факторов, влияющих на защищенность и надежность ЗКТС (ЛР2, 6 ч).
3	3	Создание классификационного перечня угроз для исследуемой лабораторной сети (ЛР3, 8 ч)
4	4	Политики безопасности в ОС Linux, ОС Windows. Ядро операционной системы (ЛР4, 8 ч)
5	5	Имплементация дискреционного доступа в ОС Linux (ЛР5, 6 ч.)
6	5	Имплементация мандатного доступа в ОС Linux (ЛР6, 4 ч.)
7	6	Создание элементов политики тематического доступа на базе ОС Linux и Qt Creator (ЛР7, 8ч)
8	7	Установка и настройка корпоративного сетевого экрана pfSense (ЛР8, 6 ч)
9	7	Установка и настройка интерактивного детектора атак (IDS) в ОС Linux (ЛР9, 4 ч)
10	8	Настройка SSL/TLS аутентификации при Web-доступе с использованием сервера Apache (ЛР10, 8 ч)

4.5 Виды и типовые темы самостоятельной работы студентов

Таблица 4.5 – Виды и типовые темы самостоятельной работы студентов (СРС)

Номер темы дисциплины	**Вид самостоятельной работы студентов**	**Трудоёмкость, часов**
1	2	3
1,2	Классификация возможных каналов утечки информации при эксплуатации узлов ЗКТС (ИТМ1)	10
3,4	Парирование типовых угроз безопасности при помощи политик безопасности различных видов (ИТМ2)	10
5,6	Сравнительный анализ дискреционной и ролевой политик безопасности (ИТМ3)	10
5,6	Сравнительный анализ мандатной и тематической политик безопасности (ИТМ4)	10
5	Построение модели безопасности на основе результатов анализа ЗКТС (ИЗПЗ1)	4
5	Создание тематической решетки на основе классификационных множеств (ИЗПЗ2)	4
5,6	Составление перечня типовых ролей пользователя и определение доступа к защищаемым объектам (ИЗПЗ3)	4
5,7	Создание ранговой шкалы компьютерных систем в пространстве шкалирования первичных факторов оценки (ИЗПЗ4)	4
1	Анализ выявленных каналов утечки информации (ИЗЛР1)	4
3	Выработка предложений по борьбе с выявленными угрозами из перечня по лабораторной сети (ИЗЛР2)	4
4	Анализ политик безопасности, реализуемых ядром ОС Linux (ИЗЛР3)	4
4	Анализ политик безопасности, реализуемых ядром ОС Windows. (ИЗЛР4)	4
5	Создание отчета о принципах имплементации мандатного и дискреционного доступа в ОС Linux (ИЗЛР5)	4
6	Создание интерфейса пользователя политики тематического доступа (ИЗЛР6)	4
7	Резервное копирование конфигураций сетевых экранов и детекторов атак. Использование шаблонов (ИЗЛР7)	4
8	Генерация самоподписанных сертификатов (ИЗЛР8)	4
1,2,3,4	Курсовая работа по изучаемой дисциплине (КР)	21
5,6,7,8	Индивидуальное комплексное задание по дисциплине (ИКЗД)	21
	Итого: в **ч** / в **ЗЕ**	**63/1,8**

4.6 Перечень тем курсовых работ (проектов)

Таблица 4.6 – Темы курсовых работ*

№ п.п.	Номер темы дисциплины	Наименование темы лабораторной работы
1	2	3
1	1,2,3,4	Комплексное обеспечение информационной безопасности лабораторной инфраструктуры с использованием ОС Windows и персональных решений
2	1,2,3,4	Комплексное кроссплатформенное обеспечение информационной безопасности многосегментной лабораторной сети для рабочих мест с ОС Linux, ОС Windows

* Приведенные темы являются базовыми для формирования индивидуальной темы курсовой работы для каждого студента

5 Образовательные технологии, используемые для формирования компетенций

Проведение лекционных занятий по дисциплине основывается на активном методе обучения, при котором учащиеся являются активными участниками занятия, отвечающие на заранее намеченный преподавателем список вопросов, стимулирующих ассоциативное мышление и установления связей с ранее освоенным материалом.

Практические занятия проводятся на основе реализации метода обучения действием: определяются проблемные области; формируются группы для их решения; каждое практическое занятие проводится по своему алгоритму.

Сформированные на практических занятиях знания и умения находят закрепление в выполнении индивидуальных заданий по их тематике.

Проведение лабораторных занятий основывается на интерактивном методе обучения, при котором учащиеся взаимодействуют не только с преподавателем, но и друг с другом. При этом доминирует активность учащихся в процессе обучения. Место преподавателя в интерактивных лабораторных занятиях – направление деятельности учащихся на достижение целей занятия.

Тематика лабораторных работ непосредственно связана с получением практических навыков по настройке и использованию комплексных средств защиты информации в инфокоммуникационных системах

Выполнение СРС по дисциплине естественным образом опирается на проектный подход к образованию, который основан на идее использования проектирования как компоненты организации обучения и как основы учебно-познавательной (учебно-профессиональной) деятельности обучающегося в рамках используемых образовательных технологий.

Реализация процесса освоения дисциплины «Безопасность сетей ЭВМ» на основе проектного подхода и широкого применения средств автоматизации проектирования при решении частных задач и комплексной задачи проектирования обеспечивает достижение обучаемыми высокого уровня освоения заданных компетенций.

6 Управление и контроль освоения компетенций

6.1 Текущий контроль освоения заданных дисциплинарных частей компетенций

Текущий контроль предназначен для оценки освоения дисциплинарных частей компетенций в ходе учебного процесса.

Текущий контроль освоения дисциплинарных компетенций проводится в следующих формах:

- выполнение тестов по материалам темы, рассмотренной на лекции;
- выполнение тестов по материалам темы, изученной самостоятельно;
- выполнение тестов по материалам практических и лабораторных работ.

6.2 Рубежный и промежуточный контроль освоения заданных дисциплинарных частей компетенций

Рубежный контроль предназначен для оценки освоения дисциплинарных частей компетенций, относящихся к одному модулю дисциплины.

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

- выполнение тестов по материалам модуля (модуль 1, 2, 3, 4);
- защита рефератов по темам модуля (модуль 1, 2, 3, 4) – РФ1, РФ2, РФ3, РФ4;
- защита отчетов по индивидуальным заданиям по теме практических занятий модуля (модуль 3, 4) – ОИЗПЗ1, ОИЗПЗ2, ОИЗПЗ3, ОИЗПЗ4;
- защита отчетов по индивидуальным заданиям по теме лабораторных работ модуля (модуль 1, 2, 3, 4) – ОЛР1, ОЛР2, ОЛР3, ОЛР4, ОЛР5, ОЛР6, ОЛР7, ОЛР8, ОЛР9, ОЛР10;

Промежуточный контроль предназначен для промежуточной оценки освоения дисциплинарных частей компетенций. Промежуточный контроль проводится в следующих формах:

- защита курсовой работы по дисциплине – КР.
- защита отчета по выполнению индивидуального комплексного задания по дисциплине – ОИКЗД.

6.3 Итоговый контроль освоения заданных дисциплинарных частей компетенций

1) **Зачёт**

«Не предусмотрен».

2) **Экзамен**

На экзамене по дисциплине студенту предлагается решить несколько теоретических и одно практическое задание.

Экзаменационная оценка выставляется с учётом результатов рубежного и промежуточного контроля.

Фонды контролирующих и измерительных (оценочных) средств, включающие тестовые задания, перечень тем рефератов, типовые индивидуальные задания к ПЗ и ЛР, вопросы и задания для экзамена, дескрипторы, индикаторы и критерии оценивания представлены отдельным документом в составе УМКД.

6.4. Формы контроля освоения компонентов дисциплинарных компетенций

Таблица 6.1. Структура учебной работы студента по видам, формам представления результатов и формам контроля

Индексы компонентов ДК	Компоненты ДК	Формулировки компонентов ДК	АРС		СРС		№ Темы
			Форма выполнения	Форма контроля	Форма представления результатов	Форма контроля	
1	2	3	4	5	6	7	8
ПК-8. С3. Б17	Знает	- основные направления развития информационно-коммуникационных технологий объекта защиты, (1з)	Л	ТК	РФ1 Тест	РК	1,2
		- методы оценки эффективности функционирования систем информационной безопасности, способы оценки затрат и рисков; (2з)	Л	ТК	РФ1 Тест	РК	1,2

1	2	3	4	5	6	7	8
		- типовые структуры, принципы организации, средства и технологии обеспечения информационной безопасности объектов защиты (3з)	Л	ТК	РФ1 Тест	РК	3,4 5,6
	Умеет	- анализировать направления развития информационно-коммуникационных технологий объекта защиты, прогнозировать эффективность функционирования систем информационной безопасности; (1у)	ПЗ1 ЛР1	ТК	ОИЗПЗ1 ОЛР1	РК	2,3
		- обосновывать выбор структуры, принципов организации, комплекса средств и технологий обеспечения информационной безопасности объектов защиты; (2у)	ПЗ2 ЛР2	ТК	ОИЗПЗ2 ОЛР2	РК	2,5
	Владеет	- навыками организации комплекса средств и технологий обеспечения информационной безопасности объектов защиты; (1в)			КР	ПК Экзамен	1,2
ПК-19. С3. Б17	Знает	- современные методы обеспечения информационной безопасности, вновь вводимые отечественные и международные стандарты; (1з)	Л	ТК	Тест	РК	4,5
		- основные угрозы информационной безопасности объектов и методы противодействия им; (2з)	Л	ТК	РФ2 Тест	РК	6,7
		- требования к архитектуре информационных систем и их компонентам для обеспечения безопасности функционирования; (3з)	Л	ТК	РФ2 Тест	РК	6,7
	Умеет	- осваивать и адаптировать к защищаемым объектам современные методы обеспечения информационной безопасности, вновь вводимые отечественные и международные стандарты; (1у)	ПЗ3 ЛР3 ЛР4	ТК	ОИЗПЗ3 ОЛР3 ОЛР4	РК	5,6
		- анализировать угрозы информационной безопасности объектов и разраба-	ПЗ4 ЛР5 ЛР6	ТК	ОИЗПЗ4 ОЛР5	РК	6,7

1	2	3	4	5	6	7	8
		тывать методы противодействия им; (2у)					
	Владеет	- навыками применения современных методов обеспечения информационной безопасности, внедрения на объекты защиты вновь вводимых и существующих отечественных и международных стандартов. (1в)			ИКЗД КР	ПК Экзамен	1,2 3,4
ПСК-07. 02.2014. С3. Б17	Знает	- нормативные документы по метрологии, стандартизации и сертификации программных и аппаратных средств защиты. (1з)	Л	ТК	Тест	РК	6
		- структуры и организацию построения узлов ЗКТС; (2з)	Л	ТК	РФ3 Тест	РК	7
		- методы обеспечения надежности ЗКТС; (3з)	Л	ТК	РФ4 Тест	РК	8
	Умеет	- использовать методы и средства определения технологической безопасности функционирования распределенной информационной системы; (1у)	ЛР7 ЛР8	ТК	ОЛР7 ОЛР8	РК	7
		- применять нормативные документы по метрологии, стандартизации и сертификации на практике. (2у)	ЛР9 ЛР10	ТК	ОЛР9 ОЛР10	РК	6,7 8
	Владеет	- навыками анализа угроз информационной безопасности объектов и разработки соответствующих методов противодействия им (1в)			ИКЗД	ПК Экзамен	5,6 7,8

Примечание: ТК – текущий контроль, РК – рубежный контроль, ПК - промежуточный контроль

7 График учебного процесса по дисциплине

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

Вид работы	Распределение по учебным неделям																		Итого
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	
Раздел:	**Р1**									**Р2**									
Л	2	4	2							4	4								**16**
ПЗ																			
ЛР						5		6							8		8		**27**
Аудиторная работа:																			**45**
КСР									1									1	**2**
ИТМ					5		5							5		5			**20**
ИЗПЗ																			
ИЗЛР							4		4					4		4			**16**
КР					3	3	3	4						3	4	3	4		**27**
Самостоятельная работа:																			**63**
Модуль:	**М1**									**М2**									
Контр. тестирование							+											+	
Дисциплин. контроль																			**Экзамен 36**
Общая трудоемкость:																			**144**

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

Вид работы	Распределение по учебным неделям																		Итого
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	
Раздел:	**Р3**									**Р4**									
Л	4	4	4	4						4	4	4	2						**32**
ПЗ					4		4					4		6					**18**
ЛР						6	4	4	4					6	4	4	4		**36**
																		Аудиторная работа:	**90**
КСР					1				1					1				1	**4**
ИТМ					5		5							5		5			**20**
ИЗПЗ						4		4							4		4		**16**
ИЗЛР							4		4					4		4			**16**
ИКЗД			5		5		4		5			5		5		5		4	**38**
																		Самостоятельная работа:	**90**
Модуль:	**М3**									**М4**									
Контр. тестирование							+											+	
Дисциплин. контроль																			**Экзамен 36**
																		Общая трудоемкость:	**216**

8 Учебно-методическое и информационное обеспечение дисциплины

8.1 Карта обеспеченности дисциплины учебно-методической литературой

Безопасность сетей ЭВМ	***Профессиональный*** (*цикл дисциплины*)
(*полное название дисциплины*)	[*x*] основная [ ] по выбору студента; [x] базовая часть цикла [ ] вариативная часть цикла

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

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

2011 (*год утверждения учебного плана ООП*)

Семестр(ы) *8,9*

Количество групп 1

Количество студентов 25

Безукладников Игорь Игоревич (*фамилия, инициалы преподавателя*) — **доцент** (*должность*)

Электротехнический (*факультет*)

Автоматика и телемеханика (*кафедра*) — **(342) 239-18-16** (*контактная информация*)

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	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	Информационная безопасность : учебное пособие / С. В. Петров [и др.] ; Новосибирский государственный педагогический университет ; Московский государственный педагогический университет .— Новосибирск ; Москва : АРТА, 2012 .— 295 с.	1
3	Информационная безопасность открытых систем : учебник / Д. А. Мельников .— Москва : Флинта : Наука, 2014 .— 442 с.	1
4	Гольдштейн Б.С. Сети связи: учеб. для вузов / Б.С. Гольдштейн, Н.А. Соколов, Г.Г. Яновский. – СПб: БХВ-Петербург, 2011. – 399 с.: ил.	2
2 Дополнительная литература		
	2.1 Учебные и научные издания	
1	Программно-аппаратные средства обеспечения информационной безопасности. Защита программ и данных : учебное пособие / П. Ю. Белкин [и др.] .— Москва : Радио и связь, 1999 .— 169 с.	17
2	Теоретические основы компьютерной безопасности : учебное пособие для вузов / П. Н. Девянин [и др.] .— Москва : Радио и связь, 2000 .— 190 с	32
3	Основы безопасности информационных систем : учебное пособие для вузов / Д. П. Зегжда, А. М. Ивашко .— Москва : Горячая линия-Телеком, 2000 .— 451 с.	18
4	Стандарты информационной безопасности : курс лекций / В. А. Галатенко ; Под ред. В. Б. Бетелина ; Интернет-университет информационных технологий ; Под ред. В. Б. Бетелина .— Москва : ИНТУИТ, 2004 .— 322 с.	12
5	Праскурин Г.А. Организационное обеспечение информационной безопасности: курс лекций. - Томск: Изд-во ТУСУР, 2005. Ч. 1. - 2005. - 221 с.	5
	2.2 Периодические издания	
	2.3Электронные образовательные ресурсы	
1	Электронная библиотека ПНИПУ http://lib.pstu.ru/	Без ограничения доступа
2	Электронно-библиотечная система «Издательство Лань» http://e.lanbook.com/books/	
3	Наукометрическая и реферативная база данных Scopus	
4	Электронная база данных WebofScience	

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

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

8.2 Компьютерные обучающие и контролирующие программы

Таблица 8.2 – Программы, используемые для обучения и контроля

№ п.п.	Вид учебного занятия	Наименование программного продукта	Рег. номер	Назначение
1	2	3	4	5
1	ЛР	Тестовая система http://test.at.pstu.ru	-	Программа предназначена для проверки знаний студентов при текущей аттестации, а также для допуска к выполнению лабораторных работ.

8.3 Аудио- и видео-пособия

Таблица 8.3 – Используемые аудио- и видео-пособия

Вид аудио-, видео-пособия				Наименование учебного пособия
теле-фильм	кино-фильм	слайды	аудио-пособие	
1	2	3	4	5
		+		Электронные лекции-презентации по дисциплине

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	Комплексные средства защиты информации	Кафедра АТ	308, ЭТФ	25	6

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	Персональный компьютер	7	собственность	308, ЭТФ

Лист регистрации изменений

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

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
«Безопасность сетей ЭВМ»
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: 4,5 **Семестр: 8,9**
Трудоемкость:
Кредитов по базовому учебному плану (БУП): **10**
Часов по базовому учебному плану (БУП): **360**

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

Пермь 2017 г.

Рабочая программа дисциплины «Безопасность сетей ЭВМ» разработана на основании:

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

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

Основы информационной безопасности, Криптографические методы защиты информации, Организационное и правовое обеспечение информационной безопасности, Управление информационной безопасностью, Вычислительная техника и информационные технологии, Основы построения инфокоммуникационных систем и сетей, Программно-аппаратные средства защиты информации, Разработка и эксплуатация защищенных автоматизированных систем.

Лист регистрации изменений

№ п.п	Содержание изменения	Дата, номер протокола заседания кафедры. Подпись заведующего кафедрой
1.	Содержание стр. 1, кроме абзацев 6-9, изложить в редакции, приведенной на стр. 1а.	Протокол заседания кафедры АТ от «16» 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-19 считать профессиональной компетенцией **ПК-12** с формулировкой: «Способность участвовать в проектировании системы управления информационной безопасностью автоматизированной системы»; - изменить шифр дисциплинарной компетенции с ПК-19-С3.Б.17 на ПК-12.Б1.Б.38; - профессиональную компетенцию ПК-8 считать профессиональной компетенцией **ПК-5** с формулировкой: «Способность проводить анализ рисков информационной безопасности автоматизированной системы»; - изменить шифр дисциплинарной компетенции с ПК-8-С3.Б.17 на ПК-5.Б1.Б.06; - профессионально-специализированную компетенцию ПСК-07.02.2014 считать компетенцией **ПСК-7.3** с формулировкой « Способность проводить аудит защищенности информационно-технологических ресурсов распределенных информационных систем» - изменить шифр дисциплинарной компетенции с ПСК-07.02.2014.С3.Б.17 на ПСК-7.3.Б1.Б.38	
	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 10 ЗЕ. Количество часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся указано в таблице 3.1.».	
	В табл. 3.1.: а) строку п. 1 дополнить словами «(контактная работа)»; б) строку п. 3 изложить в следующей редакции: «Итоговый контроль (промежуточная аттестация обучающихся) по дисциплине:».	
	В табл. 4.1.: а) в строке п. 1 «Количество часов (очная форма обучения)» дополнить словами «и виды занятий»; б) «Итоговая аттестация» заменить на «Итоговый контроль (промежуточная аттестация).	
	В раздел 4.4 «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. Пере-	

	чень основной и дополнительной учебной литературы, необходимой для освоения дисциплины».	
	Добавить в таблицу 8.1 строку «2.5 Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины».	
	Дополнить п. 2.5 таблицы строками: **Электронная библиотека** Научной библиотеки Пермского национального исследовательского политехнического университета [Электронный ресурс : полнотекстовая база данных электрон. документов изданных в Изд-ве ПНИПУ]. – Электрон. дан. (1 912 записей). – Пермь, 2014. – Режим доступа: http://elib.pstu.ru/. – Загл. с экрана. **Лань** [Электронный ресурс : электрон.-библ. система : полнотекстовая база данных электрон. документов по гуманит., естеств., и техн. наукам] / Изд-во «Лань». – Санкт-Петербург : Лань, 2010- . – Режим доступа: http://e.lanbook.com/. – Загл. с экрана. **Консультант Плюс** [Электронный ресурс : справочная правовая система : документы и комментарии : универсал. информ. ресурс]. – Версия Проф, сетевая. – Москва, 1992. – Режим доступа: Компьютер. сеть Науч. б-ки Перм. нац. исслед. политехн. ун-та, свободный.».	
	Раздел 8.2 «Компьютерные обучающие и контролирующие программы» считать 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».	