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
«Программно-аппаратные средства защиты информации»

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:	3	ЗЕ
Часов по рабочему учебному плану:	114	Ч

Виды контроля:

Экзамен: - Зачёт: **-7 сем.** 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» 01 2017 г. № 18

УЧЕБНО-МЕТОДИЧЕСКИЙ КОМПЛЕКС ДИСЦИПЛИНЫ «Программно-аппаратные средства обеспечения информационной безопасности (Программно-аппаратные средства защиты информации)»
РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

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

Курс: 4 **Семестр:** 7

Трудоемкость:
Кредитов по базовому учебному плану (БУП): **3**
Часов по базовому учебному плану (БУП): **108**

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

Пермь 2017 г.

Рабочая программа дисциплины «Программно-аппаратные средства защиты информации» 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: «Техническая защита информации», «Комплексная система защиты информации на предприятии».

Разработчик канд. техн. наук, доцент _____ Кокоулин А.Н.

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

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

Рабочая программа одобрена методической комиссией электротехнического факультета
«25» 06 2015 г., протокол № 3
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 «Программно-аппаратные средства обеспечения информационной безопасности (Программно-аппаратные средства защиты информации)» 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: Вычислительная техника и информационные технологии, Электроника и схемотехника 1 (Электроника), Электроника и схемотехника 2 (Схемотехника), Электроника и схемотехника 3 (Электропитание устройств и систем), Теория электрических цепей, Электромагнитные поля и волны, Информатика 1, Технические средства охраны, Техническая защита информации 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 разработки и эксплуатации автоматизированных систем в защищенном исполнении, отдельных компонентов автоматизированных систем, с учетом требований нормативно-технической и методической документации по обеспечению безопасности информации.

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-10	способность администрировать подсистемы информационной безопасности объекта
			ПК-11	способность к установке, настройке и эксплуатации компонентов системы защиты информации на объектах информатизации с учетом требований нормативно-технической документации
2.	090303.65	Информационная безопасность автоматизированных систем	ПК-8	способность к освоению новых образцов программных, технических средств и информационных технологий
			ПК-17	способность проводить синтез и анализ проектных решений по обеспечению безопасности автоматизированных систем

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 участвовать в разработке и администрировании защищенных автоматизированных систем по профилю своей профессиональной деятельности

Унифицированная профессиональная компетенция (УПК-2)

Способность участвовать в разработке и эксплуатации компонентов автоматизированных систем на объектах информатизации в сфере профессиональной деятельности, с учетом требований нормативно-технической документации

Таблица 1.2 Обоснование разработки унифицированных компетенций

№	Направление подготовки		Соответствие унифицированной компетенции и базовой компетенции ФГОС ВПО	
	Код	Наименование	**Способность участвовать в разработке и администрировании защищенных автоматизированных систем по профилю своей профессиональной деятельности (УПК-1)**	**Способность участвовать в разработке и эксплуатации компонентов автоматизированных систем на объектах информатизации в сфере профессиональной деятельности, с учетом требований нормативно-технической документации (УПК-2)**
1.	090900.62	Информационная безопасность	Способность администрировать подсистемы информационной безопасности объекта (ПК-10)	Способность к установке, настройке и эксплуатации компонентов системы защиты информации на объектах информатизации с учетом требований нормативно-технической документации (ПК-11)
2.	090303.65	Информационная безопасность автоматизированных систем	Способность к освоению новых образцов программных, технических средств и информационных технологий (ПК-8)	Способность проводить синтез и анализ проектных решений по обеспечению безопасности автоматизированных систем (ПК-17)

1.2. Задачи дисциплины:

- изучение основных угроз безопасности информации в автоматизированных системах и освоение методов защиты от данных угроз;
- изучение методов, алгоритмов, программно-аппаратных средств обеспечения информационной безопасности автоматизированных систем;
- изучение основных мер по защите информации и программных продуктов от несанкционированного доступа, модификации и изучения в автоматизированных системах;
- изучение современных технологий защищенных сетей передачи данных в автоматизированных системах.

После изучения дисциплины обучающийся должен демонстрировать следующие результаты:

знать:

- архитектуру и базовые принципы функционирования вычислительных систем, сетей и современных многозадачных многопользовательских операционных систем;
- виды, функции и требования к современным средствам программной и аппаратной аутентификации пользователей и программ в клиент-серверных приложениях;
- методы и программно-аппаратные средства защиты программного обеспечения от несанкционированного изучения, копирования и модификации;
- модульную структуру подсистемы безопасности современных операционных систем и способы интеграции средств защиты;
- методы и алгоритмы управления и генерации ключей и их аппаратно-программная реализация и применение в автоматизированных системах;
- принципы построения безопасных автоматизированных рабочих мест и вычислительных сетей с использованием программных и аппаратных комплексов.

уметь:

- развертывать и настраивать программные и аппаратные средства для защиты локальных и распределенных вычислительных систем;
- обеспечивать надежную аутентификацию и управление доступом к информационным ресурсам с учетом требований нормативно-технической документации;
- настраивать каналы безопасного обмена информацией в локальных и распределенных автоматизированных системах;
- настраивать системы обнаружения вторжений и антивирусные системы

владеть:

- инструментарием, обеспечивающим программно-аппаратную защиту информационных ресурсов от изучения, модификации и копирования;
- программно-аппаратными комплексами управления ключами, сертификатами и правами пользователей в защищенных автоматизированных системах.

1.3. Предметом освоения дисциплины являются следующие объекты:

- модели данных, систем и процессов защиты информации;
- программные и аппаратные средства защиты автоматизированных систем;
- угрозы безопасности информации в автоматизированных системах;
- схемы аутентификации в автоматизированных системах;
- методы и модели генерации и управления ключами;
- стадии и этапы разработки автоматизированных систем;
- методы интеграции программные и аппаратные средства защиты в информационные системы;
- методы и средства обнаружения и предотвращения вторжений;
- средства анивирусной защиты в автоматизированных системах;
- методы построения виртуальных сетей в автоматизированных системах;
- методы, способы и средства обеспечения отказоустойчивости.

1.4. Место дисциплины в структуре профессиональной подготовки выпускников

Дисциплина «Программно-аппаратные средства защиты информации» относится к вариативной части цикла профессиональных дисциплин по направлению 090900 Информационная безопасность (квалификация (степень) «бакалавр») и к базовой части цикла профессиональных дисциплин 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 участвовать в разработке и администрировании защищенных автоматизированных систем по профилю своей профессиональной деятельности	Программирование и основы алгоритмизации (методы и технологии программирования); Основы построения инфокоммуникационных систем и сетей; Вычислительная техника и информационные технологии	Комплексная защита информации на предприятии
УПК-2	Способность участвовать в разработке и эксплуатации компонентов автоматизированных систем на объектах информатизации в сфере профессиональной деятельности, с учетом требований нормативно-технической документации	Криптографические методы защиты информации; Защита и обработка конфиденциальных документов; Программирование и основы алгоритмизации (методы и технологии программирования);	Комплексная защита информации на предприятии Информационная безопасность в банковской системе

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 участвовать в разработке и администрировании защищенных автоматизированных систем по профилю своей профессиональной деятельности

Требования к компонентному составу компетенции

Перечень компонентов	Виды учебной работы	Средства оценки
В результате освоения компетенции, студент знает: – архитектуру и базовые принципы функционирования вычислительных систем, сетей и современных многозадачных многопользовательских операционных систем; – виды, функции и требования к современным средствам программной и аппаратной аутентификации пользователей и программ в клиент-серверных приложениях; – методы и программно-аппаратные средства защиты программного обеспечения от несанкционированного изучения, копирования и модификации;	Лекции Семинарские занятия Самостоятельная работа студентов по изучению теоретического материала Зачет	Вопросы текущего, рубежного и итогового контроля
умеет: – развертывать и настраивать программные и аппаратные средства для защиты локальных и распределенных вычислительных систем; – настраивать каналы безопасного обмена информацией в локальных и распределен-ных автоматизированных системах;	Практические занятия Самостоятельная работа студентов по решению практических задач	Темы индивидуальных заданий к практическим занятиям и индивидуальные задания по модулю
владеет: – инструментарием, обеспечивающим программно-аппаратную защиту информационных ресурсов от изучения, модификации и копирования	Самостоятельная работа студентов по решению практических задач Самостоятельная работа студентов по выполнению индивидуального задания	Темы индивидуальных заданий к практическим занятиям и индивидуальные задания по модулю

2.2. Дисциплинарная карта компетенции УПК-2

Код УПК-2	**Формулировка унифицированной дисциплинарной компетенции** Способность участвовать в разработке и эксплуатации компонентов автоматизированных систем на объектах информатизации в сфере профессиональной деятельности, с учетом требований нормативно-технической документации

Требования к компонентному составу компетенции

Перечень компонентов	Виды учебной работы	Средства оценки
В результате освоения компетенции, студент знает: – модульную структуру подсистемы безопасности современных операционных систем и способы интеграции средств защиты; – методы и алгоритмы управления и генерации ключей и их аппаратно-программная реализация и применение в автоматизированных системах; – принципы построения безопасных автоматизированных рабочих мест и вычислительных сетей с использованием программных и аппаратных комплексов;	Лекции Семинарские занятия Самостоятельная работа студентов по изучению теоретического материала Зачет	Вопросы текущего, рубежного и итогового контроля
умеет: – обеспечивать надежную аутентификацию и управление доступом к информационным ресурсам с учетом требований нормативно-технической документации; – настраивать системы обнаружения вторжений и антивирусные системы;	Практические занятия Самостоятельная работа студентов по решению практических задач	Темы индивидуальных заданий к практическим занятиям и индивидуальные задания по модулю
владеет: – программно-аппаратными комплексами управления ключами, сертификатами и правами пользователей в защищенных автоматизированных системах.	Самостоятельная работа студентов по решению практических задач Самостоятельная работа студентов по выполнению индивидуального задания	Темы индивидуальных заданий к практическим занятиям и индивидуальные задания по модулю

3. Объем дисциплины и виды учебной работы

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

3.2. Основными видами аудиторной работы по дисциплине являются:

- лекции (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)	**60**	
	- самостоятельное изучение теоретического материала (ИТМ)	30	отчет по вопросам для текущего и рубежного контроля
	- выполнение индивидуальных заданий по модулю (ИЗМ)	30	отчёт о выполнении
3	Итоговая аттестация по дисциплине		**Зачет**
4	**Трудоёмкость дисциплины, всего:** **в часах (ч)** **в зачётных единицах (ЗЕ)**	 **114** **3**	

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		**38,5/1**
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		4	4	2		10
		9	4,5	2	2	0,5	6	4	2		10,5
	Всего по модулю:		**20,5**	10	10	0,5	**22**	12	10		**42,5/1.1**
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		**33/0.9**
Итоговая аттестация										зачет	
Итого			**54**	**24**	**28**	**2**	**60**	**30**	**30**	**36**	**114/3**

4.2. Содержание разделов и тем учебной дисциплины

Модуль 1. Безопасность локальных вычислительных систем.
Раздел 1. Безопасность локальных вычислительных систем.
АРС: Л - 8 ч, ПЗ, СЗ - 10 ч., КСР – 0,5 ч., СРС: ИТМ - 10 ч., ИЗМ (ИЗМ-1) - 10 ч.

Тема 1. Предмет и задачи программно-аппаратной защиты информации. Цели, задачи и содержание курса. Основные понятия. Предмет и задачи программно-аппаратной защиты информации. Автоматизированная система (АС). Структура и компоненты АС. Сети ЭВМ. Электронный документ (ЭД). Виды информации в КС. Информационные потоки в КС. Уязвимость компьютерных систем. Понятие доступа, субъект и объект доступа. Понятие несанкционированного доступа (НСД). Классы и виды НСД. Несанкционированное копирование программ как особый вид НСД. Политика безопасности в компьютерных системах. Оценка защищенности. Способы защиты конфиденциальности, целостности и доступности в КС. Стандарты и рекомендации по оценке защищенности от НСД.

Тема 2. Структура и функции операционной системы как среды выполнения программных модулей АС. Архитектура ЭВМ и виды современных многопользовательских и многозадачных операционных систем. Реализация подсистемы безопасности ОС. Идентификация и аутентификация пользователей ОС. Виртуальные машины и среды выполнения. Понятие исполняемого модуля. API - программные интерфейсы. Безопасная работа программы в защищенном режиме работы процессора. "Модель клиент-сервер". Система Crypto API.

Тема 3. Разграничение ресурсов в локальных АС. Контроль доступа и разграничение доступа. Дискреционное и мандатное разграничение доступа. Пользователи и группы. Файл как объект доступа. Оценка надежности систем ограничения доступа - сведение к задаче оценки стойкости. Иерархический доступ к файлу. Понятие атрибутов доступа. Защита файловых ресурсов в ОС Windows и Unix. Способы фиксации фактов доступа. Журналы доступа. Доступ к данным со стороны процесса. Понятие доступа к данным со стороны процесса: отличия от доступа со стороны пользователя. Понятие и примеры скрытого доступа.

Тема 4. Дизассемблеры и отладчики (дебаггеры). Способы исследования программ, виды отладчиков. Ресурсы, упакованные в программном модуле. Секции программ. Трассировка программ платформы Win32 и программ, платформ .NET и Java. Патчинг программ для снятия и обхода механизмов защиты. Использование упаковщиков кода. Защита программ от отладки и изучения.

Модуль 2. Безопасность сетевых автоматизированных систем.
Раздел 3. Безопасность сетевых автоматизированных систем.
АРС: Л - 10 ч, ПЗ, СЗ - 10 ч., КСР – 0,5 ч., СРС: ИТМ - 14 ч., ИЗМ (ИЗМ-1) - 10 ч.

Тема 5. Аутентификация и идентификации пользователя. Идентификация субъекта. Понятие протокола идентификации. Локальная и удаленная идентификация. Понятие идентифицирующей информации. Способы хранения идентифицирующей информации. Связь с ключевыми системами. Программно-аппаратные средства аутентификации: биометрические, пассивные и активные устройства. Сетевая аутентификация в корпоративных системах. Управление сертификатами Kerberos. Протокол LDAP. Инфраструктура управления ключами PKI.

Тема 6. Средства программно-аппаратной защиты информации. Принципы работы и функционал СЗИ. Обеспечение безопасной загрузки операционной системы и верификация модулей. Централизованное управление. Интеграция в существующую автоматизированную систему предприятия. Средства, сертифицированные ФСТЭК. Примеры СЗИ: БлокХост, Аккорд, Соболь.

Тема 7. Электронные ключи. Структура и функционал электронных ключей. Программные модули: драйвер ключа и API ключа. Структура защищенной программы. Преимущества и ограничения ключей как методы защиты ПО от нелегального распространения. Виды защиты: конверт (envelope), триальные и ограниченные версии, интеграция API ключа в разрабатываемую программу. Способы обхода ключевой защиты: создание драйверов протоколирования и эмуляции ключа. Современные ключи с динамической защитой. Сетевые ключи.

Тема 8. Разрушающие программные воздействия. Разрушающие программные воздействия: вирусы, трояны, malware, adware. Классификация и технологии вирусов. Руткиты: вредоносное ПО для организации удаленного управления ЭВМ и создания ботнетов. Методы маскирования активности в файловой системе и в реестре, маскирование в списке процессов,

маскирование сетевой активности. Снифферы. Кейлоггеры. Сканеры портов. Структура антивируса.

Тема 9. Системы обнаружения и предотвращения вторжений. IDS/IPS. Алгоритмы интеллектуального анализа сетевой и локальной активности, выявляющие нестандартный обмен информацией. Пассивное и активное обнаружение атак. Прмеры систем предотвращения вторжений: Microsoft TMG, Snort. Интеграция IDS/IPS с антивирусами в распространенных программных пакетах обеспечения сетевой безопасности.

Модуль 3. Средства обеспечения информационной безопасности распределенных информационных систем.

Раздел 3. Средства обеспечения информационной безопасности распределенных информационных систем.

АРС: Л - 6 ч, ПЗ, СЗ - 8 ч., КСР – 1 ч., СРС: ИТМ - 8 ч., ИЗМ (ИЗМ-1) - 10 ч.

Тема 10. Виртуализация и облачные технологии. Виртуальные среды и машины: уровень интеграции виртуальной системы и совместное использование ресурсов хост-машины. Кластеры. Облачные технлогии SaaS, PaaS, IaaS и прочие. Размещение вычислительных ресурсов организации в коммерческих и свободных облачных хостингах. Экономические и правовые вопросы использования облачных технологий. Вопросы безопасности данных в виртуальных и облачных средах. Виртуальные частные сети (VPN). Программные и аппаратные средства создания VPN и VLAN.

Тема 11. Аппаратаные криптошлюзы. Аппаратаные криптошлюзы Континент и Криптон. Доступ удаленного пользователя в локальную сеть организации. Связь разбросанных филиалов организации в единую сеть. Организация межкорпоративного сетевого портала для ведения совместного проекта. Защищенный серфинг. криптографическая защита данных, передаваемых по каналам связи сетей общего пользования между составными частями VPN. Настройка приоритетов трафика. Маршрутизация трафика. Протоколирование сетевой активности. Блокировка трафика.

Тема 12. Аудит и безопасное хранение данныхавтоматизированных информационных систем. Аудит автоматизированных информационных систем. Журналы событий в операционных системах, базах данных. Обеспечение доступности и надежного хранения корпоративных данных: резервное копирование и отказоустойчивые дисковые массивы RAID. Организация хранилища данных с использованием технологий NAS, SAN. Встроенные средства обеспечения устойчивости к сбоям в файловых системах и системах управления базами данных, основанные на транзакциях.

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	Обнаружение потенциальных уязвимостей в программных системах, структура и назначение эксплойта, защита информации в автоматизированных системах (ПЗ)
2	2	Архитектура и функции многозадачной и многопользовательской операционной системы; межпроцессное взаимодействие в локальных и сетевых ОС. (СЗ)
3	3	Определение и содержание понятия угрозы безопасности информационным ресурсам системы; принципы и методы разграничения доступа к ресурсам. Обеспечение доступа программ к ресурсам. (СЗ)

4	4	Типовая программа отладки и изучения исполняемых модулей OllyDbg. (СЗ)
5	4	Изучение тестовой программы платформы Win32 в дебаггере (ПЗ)
6	5	Методы, алгоритмы и программно-аппаратные средства аутентификации и их интеграция в подсистему безопасности Windows. (СЗ)
7	6	Развертывание, настройка и тестирование СЗИ SecretNet, БлокХост, Аккорд (ПЗ)
8	7	Изучение программного комплекса защиты программ от копирования HASP, Guardian (ПЗ)
9	8	Снифферы и сканеры портов как средства изучения системы для выполнения атак и получения конфиденциальной информации. (СЗ)
10	9	Изучение функций систем предотвращения и обнаружения вторжений и технологии EMET. (СЗ)
11	10	Изучение технологий виртуализации, кластеризации и облачных технологий. (СЗ)
12	11	Программные и аппаратные комплексы криптошлюзов: сравнение эффективности. (СЗ)
13	12	Отслеживание системных событий в Windows и *nix; Программные способы записи событий в журналы Windows. (СЗ)
14	12	Проектирование автоматической системы резервного копирования (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: Класификация угроз информационной безопасности и изучение законодательной базы	2
2	ИТМ: Изучение архитектуры ЭВМ и принципов выполнения программ в Фон-Неймановской архитектуре компьютера.	2
3	ИТМ: Изучение иерархической системы разграничения доступа в файловой системе и реестре ОС Windows	2
4	ИТМ: Изучение основных команд языка Ассемблер и управления выполнением программ	4
4	ИЗМ: В соответствии с заданием для модуля 1, п.п. 4.5.1	10
5	ИТМ: Аппаратные средства аутентификации с использованием биометрических данных и смарт-карт	2
6	ИТМ: Изучение структуры типовой СЗИ Аккорд	2
7	ИТМ: Изучение способов реализации ключевой защиты	2
8	ИТМ: Изучение методов реализации руткитов средствами системного программного обеспечения DDK	2
9	ИТМ: Методы обнаружения активности вредоносного ПО	2
9	ИЗМ: В соответствии с заданием для модуля 2, п.п. 4.5.1	10
10	ИТМ: Изучение облачных технологий «Инфраструктура как сервис» и «Платформа как сервис»	2
11	ИТМ: Изучение методов и криптографических алгоритмов организации защищенных каналов	4

12	ИТМ: Методы мониторинга и аудита, выявления угроз информационной безопасности автоматизированных систем	2
12	ИЗМ: В соответствии с заданием для модуля 3, п.п. 4.5.1	10
	Итого: в **ч** / в **ЗЕ**	**60/1,7**

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

Индивидуальное задание представляет собой последовательность мероприятий по настройке системы безопасности типовых локальных и распределенных автоматизированных систем. Исследование системы и необходимые способы обеспечения ее безопасности производится в соответствии с вариантом. Требования устанавливаются относительно класса защиты автоматизированной системы от несанкционированного доступа, уровня защищенности персональных данных, особенностей автоматизированной системы, а также угроз безопасности информации, характерных для данной системы. Темы работ соответствуют последовательности изучаемых тем в модулях учебной дисциплины. Выполнение работ осуществляется в среде виртуальных машин с использованием свободно распространяемых компонентов и систем.

Раздел 1, модуль 1

Тема 1. Развертывание прототипа автоматизарованной системы в виртуальной среде на базе Windows и установка операционной системы для выявления уязвимостей и реализации атак (Kali Linux).

Тема 2. Настройка сетевого взаимодействия между виртуальными машинами и установка серверного программного обеспечения на изучаемую машину.

Тема 3. Настройка локальной безопасности Windows и настройка разграничения доступа к файловым ресурсам и реестру.

Тема 4. Изучение тестового приложения в отладчике и применение патча.

Раздел 2, модуль 2

Тема 5. Настройка в виртуальной машине Active Directory и изучение LDAP. Изучение технологии RDP: удаленного рабочего стола.

Тема 6. Изучение автоматизированной системы с помощью сканера уязвимостей Nessus и выполение эксплойтов. Поиск методов устранения уязвимостей (патчей).

Тема 7. Установка демоверсии комплекса HASP и защита простой программы с помощью ключа.

Тема 8. Настройка антивируса, настройка параметров автозапуска сменных носителей, настройка прав доступа к веткам реестра, отвечающим за автоматический старт программ.

Тема 9. Настройка системы предотвращения вторжений Snort.

Раздел 3, модуль 3

Тема 10. Размещение образа автоматизированной системы в бесплатном хостинге и проверка настроек безопасности с помощью сканера портов.

Тема 11. Настройка программной VPN между удаленными системами.

Тема 12. Средства аудита и обеспечения отказоустойчивости автоматизированной системы.

.

4.5.2 Перечень тем курсовых работ (проектов)

Не предусмотрены.

5 Образовательные технологии, используемые для формирования компетенций

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

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

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) **Зачет**

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

Зачет 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	Зач.
В результате освоения дисциплины студент					
Знает:					
– архитектуру и базовые принципы функционирования вычислительных систем, сетей и современных многозадачных многопользовательских операционных систем;	+	+	+		+
– виды, функции и требования к современным средствам программной и аппаратной аутентификации пользователей и программ в клиент-серверных приложениях;	+	+	+		+
– методы и программно-аппаратные средства защиты программного обеспечения от несанкционированного изучения, копирования и модификации;	+	+	+		+
– модульную структуру подсистемы безопасности современных операционных систем и способы интеграции средств защиты;	+	+	+		+
– методы и алгоритмы управления и генерации ключей и их аппаратно-программная реализация и применение в автоматизированных системах;	+	+	+		+
– принципы построения безопасных автоматизированных рабочих мест и вычислительных сетей с использованием программных и аппаратных комплексов.	+	+	+		+
Умеет:					
– развертывать и настраивать программные и аппаратные средства для защиты ло-кальных и распределенных вычислительных систем;			+	+	
– обеспечивать надежную аутентификацию и управление доступом к информацион-ным ресурсам с учетом требований нормативно-технической документации;			+	+	
– настраивать каналы безопасного обмена информацией в локальных и распределен-ных автоматизированных системах;			+	+	
– настраивать системы обнаружения вторжений и антивирусные системы			+	+	
Владеет:					
– инструментарием, обеспечивающим программно-аппаратную защиту информационных ресурсов от изучения, модификации и копирования;			+	+	
– программно-аппаратными комплексами управления ключами, сертификатами и правами пользователей в защищенных автоматизированных системах			+	+	

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);

Зач. – (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		**30**
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																			**Зач.**

8. Учебно-методическое и информационное обеспечение дисциплины

8.1. Карта обеспеченности дисциплины учебно-методической литературой

Программно-аппаратные средства защиты информации	*Профессиональный цикл*	
полное название дисциплины	[x] обязат [ ] по выбору студента	[x] базовая часть цикла [x] 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/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

Кокоулин Андрей Николаевич, доцент,
электротехнический факультет,
кафедра АТ, телефон: 239-18-16.

СПИСОК ИЗДАНИЙ

№	Библиографическое описание	Количество экземпляров в библиотеке
1	2	3
	1. Основная литература	
1	Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей: учебное пособие / В.Ф. Шаньгин.— М.: ФОРУМ: ИНФРА-М, 2008.— 415 с.	10
2	Безукладников И.И. Проектирование и эксплуатация автоматизированных систем диспетчерского управления объектами критической инфраструктуры современного города: учебное пособие для вузов / И. И. Безукладников, Е. Л. Кон, А. А. Южаков; Пермский национальный исследовательский политехнический университет.— Пермь : Изд-во ПНИПУ, 2012 .— 174 с.	5 + ЭБ
3	Громов Ю.Ю. Информационная безопасность и защита информации : учебное пособие для вузов / Ю. Ю. Громов [и др.] .— Старый Оскол : ТНТ, 2010 .— 383 с. : ил	4 5
4	Клейменов С.А. Администрирование в информационных системах : учебное пособие для вузов / С.А. Клейменов, В.П. Мельников, А.М. Петраков ; Под ред. В.П. Мельникова.— М. : Академия, 2008. — 271 с.	5
	2. Дополнительная литература	
	2.1. Учебные и научные издания	
1	Бабаш А.В. Информационная безопасность. Лабораторный практикум : учебное пособие для вузов / А. В. Бабаш, Е. К. Баранова, Ю. Н. Мельников .— Москва : КНОРУС, 2012 .— 131 с., 8,5 усл. печ. л. : ил. + CD-ROM .	2
2	Гаврилов М,В. Информатика и информационные технологии : учебник для бакалавров / М. В. Гаврилов, В. А. Климов .— 2-е изд., испр. и доп .— Москва : Юрайт, 2012 .— 350 с., 18,38 усл. печ. л. : ил .— (Бакалавр) .— Библиогр.: с. 350	3
3	Дшхунян, В.Л. Электронная идентификация. Бесконтактные электронные идентификаторы и смарт-карты / В. Л. Дшхунян, В. Ф. Шаньгин .— Москва : АСТ, 2004 .— 695 с. : ил.	1 2

Основные данные об обеспеченности на _____

(дата составления рабочей программы)

Основная литература [x] обеспечена [ ] не обеспечена

Дополнительная литература [x] обеспечена [x] 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

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	321 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 IV CPU	12	Оперативное управление	321 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» 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-8 считать профессиональной компетенцией **ПК-10,** с формулировкой «Способностью применять знания в области электроники и схемотехники, технологий, методов и языков программирования, технологий связи и передачи данных при разработке программно-аппаратных компонентов защищенных автоматизированных систем в сфере профессиональной деятельности»; - изменить шифр дисциплинарной компетенции с ПК-8.С3.Б.13 на ПК-10. Б1.Б.34 - профессиональную компетенцию ПК-17 считать профессиональной компетенцией **ПК-13** с формулировкой «Способностью участвовать в проектировании средств защиты информации автоматизированной системы»; - изменить шифр дисциплинарной компетенции с ПК-17. С3.Б.13 на ПК- 13.Б1.Б.34	
	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 3 ЗЕ. Количество часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных заня-	

	тий) и на самостоятельную работу обучающихся указано в таблице 3.1.».	
	В табл. 3.1.: а) строку п. 1 дополнить словами «(контактная работа)»; б) строку п. 3 изложить в следующей редакции: «Итоговый контроль (промежуточная аттестация обучающихся) по дисциплине:».	
	В табл. 4.1.: а) в строке п. 1 «Количество часов (очная форма обучения)» дополнить словами «и виды занятий»; б) «Итоговая аттестация» заменить на «Итоговый контроль (промежуточная аттестация).	
	В раздел 4.4 «Распределение тем по видам самостоятельной работы» добавить параграф с наименованием «Методические указания для обучающихся по изучению дисциплины» следующего содержания: «При изучении дисциплины обучающимся целесообразно выполнять следующие рекомендации: 1. Изучение учебной дисциплины должно вестись систематически. 2. После изучения какого-либо раздела по учебнику или конспектным материалам рекомендуется по памяти воспроизвести основные термины, определения, понятия раздела. 3. Особое внимание следует уделить выполнению отчетов по практическим занятиям, лабораторным работам и индивидуальным комплексным заданиям на самостоятельную работу. 4. Изучение дисциплины осуществляется в течение одного семестра, график изучения дисциплины приводится п. 7. 5. Вся тематика вопросов, изучаемых самостоятельно, задается на лекциях преподавателем. Им же даются источники (в первую очередь вновь изданные в периодической научной литературе) для более детального понимания вопросов, озвученных на лекции.»	
	Наименование раздела 6 изложить в следующей редакции: «Фонд оценочных средств дисциплины».	
	Наименование параграфа 6.1 изложить в редакции «Текущий и рубежный контроль освоения заданных дисциплинарных частей компетенций».	
	В параграф 6.1 добавить первый абзац следующего содержания: «Текущий контроль осуществляется путем устного опроса во время аудиторных занятий».	
	Наименование раздела 8 Учебно-методическое и информационное обеспечение дисциплины» изложить в следующей редакции: «Перечень учебно-методического и информационного обеспечения для самостоятельной работы обучающихся по дисциплине».	
	Изменить название раздела «Список изданий» на «8.2. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины».	
	Добавить в таблицу 8.1 строку «2.5 Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины».	

	Дополнить п. 2.5 таблицы строками: **Электронная библиотека** Научной библиотеки Пермского национального исследовательского политехнического университета [Электронный ресурс : полнотекстовая база данных электрон. документов изданных в Изд-ве ПНИПУ]. – Электрон. дан. (1 912 записей). – Пермь, 2014. – Режим доступа: http://elib.pstu.ru/. – Загл. с экрана. **Лань** [Электронный ресурс : электрон.-библ. система : полнотекстовая база данных электрон. документов по гуманит., естеств., и техн. наукам] / Изд-во «Лань». – Санкт-Петербург : Лань, 2010- . – Режим доступа: http://e.lanbook.com/. – Загл. с экрана. **Консультант Плюс** [Электронный ресурс : справочная правовая система : документы и комментарии : универсал. информ. ресурс]. – Версия Проф, сетевая. – Москва, 1992. – Режим доступа: Компьютер. сеть Науч. б-ки Перм. нац. исслед. политехн. ун-та, свободный.».	
	Раздел 8.2 «Компьютерные обучающие и контролирующие программы» считать раздел 8.3 и наименование изложить в следующей редакции: «Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине».	
	Раздел 8.3 «Программные инструментальные средства» считать раздел 8.4 «Перечень программного обеспечения, в том числе компьютерные обучающие и контролирующие программы».	
	Раздел 8.4 «Аудио- и видео-пособия» считать разделом 8.5.	
	Наименование раздела 9 изложить в следующей редакции: «Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине».	
2.		
3.		
4.		
5.		