УОП

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
Проректор по учебной работе
д-р техн. наук
_____ Н. В. Лобов
«17» 04 2017 г.

УЧЕБНО-МЕТОДИЧЕСКИЙ КОМПЛЕКС ДИСЦИПЛИНЫ
«Методы проектирования защищенных распределенных систем»

Основная образовательная программа специалитета

Специальность 10.05.03 «Информационная безопасность автоматизированных систем»

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Специализация подготовки: Обеспечение информационной безопасности распределенных информационных систем

Квалификация: Специалист по защите информации

Выпускающая кафедра: «Автоматика и телемеханика»

Форма обучения: Очная

Курс: 5 **Семестр(ы):** 9

Трудоёмкость:
Кредитов по рабочему учебному плану: 3 ЗЕ
Часов по рабочему учебному плану: 108 ч

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

Пермь
2017

Рабочая программа дисциплины Методы проектирования защищенных распределенных систем 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:

Технические средства охраны, защита и обработка конфиденциальных документов, Организация и управление службой защиты информации на предприятии, Технология построения защищенных распределенных приложений - программы специалитета по направлению 10.05.03 Информационная безопасность автоматизированных систем, специализация «Обеспечение информационной безопасности распределенных информационных систем».

Разработчик
ассистент _____ А.Н. Каменских

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

Рабочая программа рассмотрена и одобрена на заседании кафедры «Автоматика и телемеханика «16» января 2016 г., протокол № 18.

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

Рабочая программа одобрена методической комиссией электротехнического факультета «5» 12 2016 г., протокол № 11.

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 – освоение дисциплинарных компетенций, связанных с созданием и изучением современных распределенных защищенных информационных систем различного применения и степени сложности.

В процессе изучения данной дисциплины студент осваивает части следующих компетенций:

1. ПСК-7.1.Б1.Б46 – способность разрабатывать и исследовать модели информационно-технологических ресурсов, разрабатывать модели угроз и модели нарушителя информационной безопасности в распределенных информационных системах.
2. ПСК-7.5.Б1.Б46 – способность координировать деятельность подразделений и специалистов по защите информации в организациях, в том числе на предприятии и в учреждении.

1.2 Задачи дисциплины:

- **Изучение** этапов и технологий проектирования и создания безопасных распределенных информационных систем; классификации средств защиты информации в корпоративных вычислительных сетях и системах; инструментальных программных и аппаратных средств анализа их защищенности.
- Формирование **умений** в разработке проектов комплексных защищенных инфраструктур для типовых современных применений, отвечающую предъявляемым требованиям к уровню защищенности, выполняемых с использованием современных программных, программно-аппаратных и аппаратных средств защиты информации.
- **Овладение** навыками разработки и внедрения комплексной защищенной инфраструктуры на предприятиях, включающих навыки базовой и расширенной настройки и использования современных программных и аппаратных средств защиты информации: файрволлов, интерактивных детекторов атак, защищенных доменных сервисов.

1.3 Предметом освоения дисциплины являются следующие объекты:

- методы и средства защиты информации в корпоративных вычислительных сетях и системах;
- основные угрозы информации в современных сложных сетевых информационных системах;
- программные, программно-аппаратные и аппаратные средства защиты информации, применяемые при обеспечении комплексной информационной безопасности;
- программные средства анализа текущего уровня защищенности;
- современные технологии построения безопасных информационных систем и сетей.

1.4 Место учебной дисциплины в структуре образовательной программы

Дисциплина «Методы проектирования защищенных распределенных систем» относится к базовой (обязательной) части цикла Блок 1 (Б1). Дисциплины (Модули).

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

- **знать:**
  - основные угрозы информации в информационных системах и сетях; современные программные и аппаратные средства криптографической защиты информации;
  - современную классификацию средств защиты информации в корпоративных вычислительных сетях и системах; этапы и технологию проектирования и создания безопасных информационных систем;
  - современную нормативно-правовую базу создания защищенных распределенных информационных систем;
  - инструментальные программные и аппаратные средства анализа защищенности информационных систем и сетей.

- **уметь:**
  - проектировать комплексную защищенную инфраструктуру для типовых современных применений, отвечающую предъявляемым требованиям к уровню защищенности;
  - разрабатывать модели информационно-технологических ресурсов, модели угроз и модели нарушителя информационной безопасности в распределенных информационных системах;
  - применять современные программные средства криптографической защиты информации; применять современные аппаратные средства защиты информационных процессов в компьютерных системах;
  - применять современные аппаратные средства защиты информационных процессов при аудите распределенных компьютерных систем.

- **владеть:**
  - навыками разработки комплексной инфраструктуры защищенной информационной системы;
  - навыками работы с ведущими программными и аппаратными комплексными средствами защиты информации.

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			
ПСК-7.1	Способность разрабатывать и исследовать модели информационно-технологических ресурсов, разрабатывать модели угроз и модели нарушителя информационной безопасности в распределенных информационных системах.	Технические средства охраны, защита и обработка конфиденциальных документов.	Технология построения защищенных распределенных приложений.
ПСК-7.5	Способность координировать деятельность подразделений и специалистов по защите информации в организациях, в том числе на предприятии и в учреждении.	Организация и управление службой защиты информации на предприятии.	-

2 Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

Учебная дисциплина обеспечивает формирование части компетенций ПСК-7.1 и ПСК-7.5.

2.1 Дисциплинарная карта компетенции ПСК-7.1

Код	Формулировка компетенции
ПСК-7.1	Способность разрабатывать и исследовать модели информационно-технологических ресурсов, разрабатывать модели угроз и модели нарушителя информационной безопасности в распределенных информационных системах.

Код	Формулировка дисциплинарной части компетенции
ПСК-7.1	Способность разрабатывать и исследовать модели информационно-технологических ресурсов, разрабатывать модели угроз и модели нарушителя информационной безопасности в распределенных информационных системах.

Требования к компонентному составу части компетенции

Перечень компонентов	Виды учебной работы	Средства оценки

В результате освоения дисциплинарной части компетенции студент **Знает:** - основные угрозы информации в информационных системах и сетях; современные программные и аппаратные средства криптографической защиты информации; - инструментальные программные и аппаратные средства анализа защищенности информационных систем и сетей.	Лекции. Самостоятельная работа студентов по изучению теоретического материала.	Тестовые вопросы текущего и рубежного контроля.
Умеет: - проектировать комплексную защищенную инфраструктуру для типовых современных применений, отвечающую предъявляемым требованиям к уровню защищенности; - разрабатывать модели информационно-технологических ресурсов, модели угроз и модели нарушителя информационной безопасности в распределенных информационных системах.	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 разработки комплексной инфраструктуры защищенной информационной системы.	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 ПСК-7.5

Код	**Формулировка компетенции**
ПК-7.5	Способность координировать деятельность подразделений и специалистов по защите информации в организациях, в том числе на предприятии и в учреждении.

Код	**Формулировка дисциплинарной части компетенции**
ПК-7.5	Способность координировать деятельность подразделений и специалистов по защите информации в организациях, в том числе на предприятиях и в учреждениях эксплуатирующих распределенные информационные системы.

Требования к компонентному составу части компетенции

Перечень компонентов	**Виды учебной работы**	**Средства оценки**

В результате освоения дисциплинарной части компетенции студент **Знает:** - современную классификацию средств защиты информации в корпоративных вычислительных сетях и системах; этапы и технологию проектирования и создания безопасных информационных систем; - современную нормативно-правовую базу создания защищенных распределенных информационных систем.	Лекции. Самостоятельная работа студентов по изучению теоретического материала.	Тестовые вопросы текущего и рубежного контроля.
Умеет: - применять современные программные средства криптографической защиты информации; применять современные аппаратные средства защиты информационных процессов в компьютерных системах; - применять современные аппаратные средства защиты информационных процессов при аудите распределенных компьютерных систем.	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 работы с ведущими программными и аппаратными комплексными средствами защиты информации.	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

Объем дисциплины в зачетных единицах составляет 3 ЗЕ. Количество часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся указано в таблице 3.1

Таблица 3.1 – Объём и виды учебной работы

№ п.п.	Виды учебной работы	Трудоёмкость	
		по семестрам	всего
1	2	3	4
1	**Контактная работа / Аудиторная работа / в том числе в интерактивной форме**	**54/54**	**54/54**
	Лекции (Л) / в том числе в интерактивной форме	16/16	16/16
	Практические занятия (ПЗ) / в том числе в интерактивной форме	18/18	18/18
	Лабораторные работы (ЛР)	18/18	18/18
2	**Контроль самостоятельной работы (КСР)**	**2**	**2**
	Самостоятельная работа студентов (СРС)	**54**	**54**
	Изучение теоретического материала (ИТМ)	10	10
	Выполнение индивидуальных заданий по тематике практических занятий (ИЗПЗ)	8	8
	Выполнение индивидуальных заданий по тематике лабораторных работ (ИЗЛР)	8	8
	Курсовой проект (КП)	28	28
4	**Итоговый контроль (промежуточная аттестация)**	**зачёт**	**зачёт**
5	**Трудоёмкость дисциплины** **Всего:** **в часах (ч)** **в зачётных единицах (ЗЕ)**	 **108** **3**	 **108** **3**

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	Итоговый контроль	самостоятельная работа	
			всего	Л	ПЗ	ЛР				
1	2	3	4	5	6	7	8	9	10	11
1	1	Введение	2	2						**2**
		1	14	4	6	4			ИТМ-4 ИЗЛР-2 ИЗПЗ-2 КП-8	**30**
		2	11	2	4	4	1		ИТМ-2 ИЗПЗ-2 ИЗЛР-2 КП-6	**23**
	Всего по модулю:		**27**	**8**	**10**	**8**	**1**		**28**	**55/1,5**
2	2	3	14	4	4	6			ИТМ-2 ИЗПЗ-2 ИЗЛР-2 КП-8	**28**
		4	11	2	4	4	1		ИТМ-2 ИЗПЗ-2 ИЗЛР-2 КП-6	**23**
		Заключение	2	2						**2**
	Всего по модулю:		**27**	**8**	**8**	**10**	**1**		**26**	**53/1,5**
Итоговый контроль (промежуточная аттестация)										**-**
Итого:			**54**	**16**	**18**	**18**	**2**		**54**	**108/3**

4.2 Содержание разделов и тем учебной дисциплины

Модуль 1 (Раздел 1). Проектирование защищенных распределенных информационных систем

Л – 8 ч, ПЗ – 10 ч, ЛР – 8 ч, СРС – 26 ч, КСР – 1 ч.

Введение

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

Тема 1. Локализация задачи комплексного обеспечения безопасности

Локализация задачи. Положение о конфиденциальной информации в электронном виде. Контентная категоризация. Классификация информации по уровню конфиденциальности. Метки документов. Хранение информации. Способы хранения конфиденциальной информации. Сводная информация. Интеллектуальная собственность. Неструктурированная информация. Локальные копии.

Тема 2. Основные направления защиты информации. Классификация внутренних нарушителей

Основные направления защиты. Защита документов. Защита каналов утечки. Мониторинг (аудит) действий пользователей. Классификация внутренних нарушителей. Неосторожные. Манипулируемые. Саботажники. Нелояльные. Нарушители, мотивированные извне. Другие типы нарушителей.

Модуль 2 (Раздел 2). Технические механизмы и средства обеспечения информационной безопасности защищенных распределенных информационных систем.

Л – 8 ч, ПЗ – 8 ч, ЛР – 10 ч, СРС – 26 ч, КСР – 1 ч.

Тема 3. Технологии аутентификации и шифрования

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. Firewall прикладного уровня для web — ModSecurity. Взаимодействие ModSecurity с пакетным фильтром.

Тема 4. Реализация комплексной безопасной распределенной сетевой инфраструктуры на примере web-сервера

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.

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	2	Классификация внутренних нарушителей. Неосторожные. Манипулируемые. Саботажники. Нелояльные. Нарушители, мотивированные извне (ПЗ1, 6 ч)
2	3	Аутентификация, основанная на IP-адресе. Basic-аутентификация. Digest-аутентификация. SSL/TLS (ПЗ2, 4 ч)
3	3	Нетехнические меры защиты от внутренних угроз (ПЗ3, 4 ч)
4	4	Классификация инструментальных средств анализа уязвимостей. (ПЗ5, 4 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	1,2	Развертывание интерактивных детекторов атак на виртуально-физической инфраструктуре XenServer (ЛР1, 4 ч).
2	1,2	Запуск и настройка защищенного web-сервера на основе пакета LAMP (ЛР2, 4 ч).
3	3,4	Создание сценариев в скриптовой среде Nessus (ЛР3, 6 ч)
4	3,4	Развертывание и настройка средства комплексной проверки сетевых уязвимостей Nessus (ЛР4, 4 ч)

5 Методические указания для обучающихся по изучению дисциплины

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.

5.1 Виды самостоятельной работы студентов

Таблица 5.1 – Виды и типовые темы самостоятельной работы студентов (СРС)

Номер темы дисциплины	Вид самостоятельной работы студентов	Трудоёмкость, часов
1	2	3
1	Контентная категоризация. Классификация информации по уровню конфиденциальности. Метки документов (ИЗП31)	2
3	Обеспечение безопасности технологий создания активного содержимого. URLs и cookies. (ИЗП32)	2
2	Обеспечение безопасности технологий создания активного содержимого. URLs и cookies. (ИЗП33)	2
4	Основные направления защиты. Защита документов. Защита каналов утечки. Мониторинг (аудит) действий пользователей. Классификация внутренних нарушителей. (ИЗП34)	2
1,2	Нетехнические меры защиты от внутренних угроз. Психологические меры. Организационные меры (ИТМ1)	5
1,3	Персональные firewall'ы и персональные устройства firewall'а (ИТМ2)	5
1,2	Авторитетные name-серверы. Кэширующие name-серверы. Resolver'ы. (ИЗЛР1)	2
2	Системы Honey Pot и Padded Cell. Выбор IDS. Определение окружения IDS. (ИЗЛР2)	2
3	Требования к аутентификации и шифрованию. Аутентификация, основанная на IP-адресе. (ИЗЛР3)	2
4	Автоматизированные инструментальные средства анализа лог-файлов (ИЗЛР4)	2
1,2,3,4	Курсовой проект по изучаемой дисциплине (КР)	28
	Итого: в **ч** / в **ЗЕ**	**54/1,5**

5.2 Перечень тем курсовых работ (проектов)

Таблица 5.2 – Темы курсовых проектов*

№ п.п.	Номер темы дисциплины	Наименование темы лабораторной работы
1	2	3
1	1,2,3,4	Создание защищенной распределенной инфраструктуры на базе ОС Windows, с использованием ПО Comodo Firewall
2	1,2,3,4	Создание защищенной инфраструктуры на базе ОС Unix Freebsd, с использованием ПО OpenBSD PF

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

5.3 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 «Методы проектирования защищенных распределенных систем» 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 Фонд оценочных средств дисциплины

6.1 Текущий и рубежный контроль освоения заданных дисциплинарных частей компетенций

Текущий контроль осуществляется путем 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;
- устный опрос во время аудиторных занятий.

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);
- защита отчетов по индивидуальным заданиям по теме практических и лабораторных занятий модуля (модуль 1, 2) – ОИЗ1, ОИЗ2, ОИЗ3, ОИЗ4.

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

- защита курсового проекта по дисциплине – КП.

6.3 Итоговый контроль освоения заданных дисциплинарных частей компетенций

1) **Зачёт**

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

Зачет выставляется с учётом результатов рубежного контроля.

2) **Экзамен**

«Не предусмотрен».

Фонды контролирующих и измерительных (оценочных) средств, включающие тестовые задания, перечень тем рефератов, типовые индивидуальные задания к ПЗ и ЛР, вопросы и задания для зачета, 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

Контролируемые результаты обучения по дисциплине (ЗУВы)	**Вид контроля**			
	Текущий и промежуточный		**Рубежный**	**Итоговый контроль**
	ПЗ	**ЛР**	**РК**	**Зачет**
Усвоенные знания				
3.1 основные угрозы информации в информационных системах и сетях; современные программные и аппаратные средства криптографической защиты информации.	С	С	ОИЗ1	ТВ

З.2 современную классификацию средств защиты информации в корпоративных вычислительных сетях и системах; этапы и технологию проектирования и создания безопасных информационных систем.	С	С	ОИЗ2	
З.3 современную нормативно-правовую базу создания защищенных распределенных информационных систем.	С	С	ОИЗ1	
З.4 инструментальные программные и аппаратные средства анализа защищенности информационных систем и сетей.	С	С	ОИЗ1	
Освоенные умения				
У.1 проектировать комплексную защищенную инфраструктуру для типовых современных применений, отвечающую предъявляемым требованиям к уровню защищенности.	КСР, ПЗ	КСР	ОИЗ3	ПЗ
У.2 разрабатывать модели информационно-технологических ресурсов, модели угроз и модели нарушителя информационной безопасности в распределенных информационных системах.	КСР, ПЗ	КСР	ОИЗ4	
У.3 применять современные программные средства криптографической защиты информации; применять современные аппаратные средства защиты информационных процессов в компьютерных системах.	КСР, ПЗ	КСР	ОИЗ3	
У.4 применять современные аппаратные средства защиты информационных процессов при аудите распределенных компьютерных систем.	КСР, ПЗ	КСР	ОИЗ4	
Приобретенные владения				
В.1 навыками разработки комплексной инфраструктуры защищенной информационной системы;			ОИЗ1	КП
В.2 навыками работы с ведущими программными и аппаратными комплексными средствами защиты информации.			ОИЗ1 ОИЗ2 ОИЗ3	

Примечание: *КСР – контроль самостоятельной работы, С – собеседование; ТВ – теоретический вопрос экзамена; ПЗ – практическое задание*

7 График учебного процесса по дисциплине

Таблица 7.1 – График учебного процесса по дисциплине

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	2	2							**16**
ПЗ				6			4						4			4			**18**
ЛР						4		4							6		4		**18**
																		Аудиторная работа:	**54**
КСР									1									1	**2**
ИТМ					4		2							2		2			**10**
ИЗПЗ				2		2							2		2				**8**
ИЗЛР							2		2					2		2			**8**
КП					5			5			4		4		5		5		**28**
																		Самостоятельная работа:	**54**
Модуль:	**М1**									**М2**									
Контр. тестирование									+									+	
Дисциплин. контроль																			**Зачет**
																		Общая трудоемкость:	**108**

8.3. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине

8.3.1 Перечень программного обеспечения, в том числе компьютерные обучающие и контролирующие программы

Таблица 8.1 – 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.

8.4 Аудио- и видео-пособия

Таблица 8.2 – 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 Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

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		

8 Перечень учебно-методического и информационного обеспечения для самостоятельной работы обучающихся по дисциплине

8.1 Карта обеспеченности дисциплины учебно-методической литературой

Б.1.Б.46 Методы проектирования защищенных распределенных систем	***Блок 1. Дисциплины (Модули)*** (*цикл дисциплины*)	
(*полное название дисциплины*)	[*X*] основная / [ ] по выбору студента	[X] базовая часть цикла / [ ] вариативная часть цикла

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

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

2017 (*год утверждения учебного плана ООП*) Семестр(ы) *9*

Количество групп 1

Количество студентов 25

Каменских Антон Николаевич (*фамилия, инициалы преподавателя*) **ассистент** (*должность*)

Электротехнический (*факультет*)

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

8.2. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

№	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 открытых систем : учебник / Д. А. Мельников .— Москва : Флинта : Наука, 2013 .— 442 с.	11
3	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	30
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, 2006 .— 322 с.	19
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	
1	Вестник ПНИПУ. Электротехника, информационные технологии, системы управления.	
	2.3 Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины	
1	Электронная библиотека Пермского национального исследовательского политехнического университета [Электронный ресурс] : [полнотекстовая база данных электрон. док., издан. в Изд-ве ПНИПУ] / Перм. нац. исслед. политехн. ун-т, Науч. б-ка. – Пермь, 2016. – Режим доступа: http://elib.pstu.ru, свободный. – Загл. с экрана.	Без ограничения доступа
2	Электронно-библиотечная система Издательство «Лань» [Электронный ресурс] : [полнотекстовая база данных : электрон. версии кн., журн. по гуманит., обществ., естеств. и техн. наукам] / Электрон.-библ. система «Изд-ва «Лань». – Санкт-Петербург, 2010-2016. – Режим доступа: http://e.lanbook.com, по IP-адресам компьютер. сети Перм. нац. исслед. политехн. ун-та. – Загл. с экрана.	

3	Scopus [Электронный ресурс] : [мультидисциплинар. реф.-библиограф. и наукометр. база данных на англ. яз.] / Elsevier B. V. – Amsterdam, 2016. – Режим доступа: http://www.scopus.com, по IP-адресам компьютер. сети Перм. нац. исслед. политехн. ун-та. – Загл. с экрана.	
4	Научная электронная библиотека eLIBRARY.RU [Электронный ресурс] : [полнотекстовая база данных : мультидисциплинар. электрон. версии журн. на ин. яз.] / Науч. электрон. б-ка. – Москва, 2000-2016. – Режим доступа: http://elibrary.ru, по IP-адресам компьютер. сети Перм. нац. исслед. политехн. ун-та. – Загл. с экрана.	

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

Карта книго-
обеспеченности
в библиотеку сдана