ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ОРЕНБУРГСКИЙ ГОСУДАРСТВЕННЫЙ АГРАРНЫЙ УНИВЕРСИТЕТ»

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.В.ДВ.06.01 Технология защиты информации в различных отраслях деятельности

Специальность 10.05.03 Информационная безопасность автоматизированных систем

Специализация Информационная безопасность автоматизированных систем критически важных объектов

Квалификация выпускника специалист

Форма обучения очная

1. Цели освоения дисциплины:

- освоение студентами знаний в области теоретической и технической защиты информации.

2. Место дисциплины в структуре образовательной программы

Дисциплина «Технология защиты информации в различных отраслях деятельности» относится к вариативной части. Требования к предшествующим знаниям представлены в таблице 2.1. Перечень дисциплин, для которых дисциплина «Технология защиты информации в различных отраслях деятельности» является основополагающей, представлен в табл. 2.2.

Таблица 2.1. Требования к пререквизитам дисциплины

Компетенции	Дисциплина
ПК-3	Безопасность операционных систем Безопасность систем баз данных Теория автоматов
ПК-8	Курс полного общего школьного образования. Информатика.
ПК-9	Курс полного общего школьного образования. Информатика.
ПК-11	Основы информационной безопасности
ПК-12	Управление информационной безопасностью
ПК-13	Курс полного общего школьного образования. Информатика.
ПК-14	Учебная практика (практика по получению первичных профессиональных умений, в том числе первичных умений и навыков научно-исследовательской деятельности) Криптографические методы защиты информации Метрология и электро-радиоизмерения
ПК-17	Техническая защита информации
ПК-19	Управление информационной безопасностью
ПК-21	Курс полного общего школьного образования. Информатика.
ПК-22	Основы информационной безопасности
ПК-23	Курс полного общего школьного образования. Информатика.
ПК-27	Курс полного общего школьного образования. Информатика.

Таблица 2.2. Требования к постреквизитам дисциплины

Компетенции	Дисциплина
ПК-3	Производственная научно-исследовательская работа Производственная (преддипломная) практика Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты (работа специалиста)
ПК-8	Производственная (преддипломная) практика Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты (работа специалиста)
ПК-9	Производственная (преддипломная) практика Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты (работа специалиста)
ПК-11	Производственная (преддипломная) практика Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты (работа специалиста)
ПК-12	Управление информационной безопасностью Производственная (преддипломная) практика Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты (работа специалиста)
ПК-13	Производственная (преддипломная) практика Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты (работа специалиста)
ПК-14	Производственная практика по получению профессиональных умений и опыта профессиональной деятельности Производственная (преддипломная) практика Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты (работа специалиста)Системы предотвращения утечек
ПК-17	Производственная практика по получению профессиональных умений и опыта профес-

	сиональной деятельности Производственная (преддипломная) практика Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты (работа специалиста)
ПК-19	Управление информационной безопасностью Производственная (преддипломная) практика Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты (работа специалиста)
ПК-21	Организационное и правовое обеспечение информационной безопасности Производственная (преддипломная) практика Выпускная квалификационная работа (работа специалиста)
ПК-22	Производственная (преддипломная) практика Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты (работа специалиста)
ПК-23	Организационное и правовое обеспечение информационной безопасности Производственная (преддипломная) практика Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты (работа специалиста)
ПК-27	Производственная практика по получению профессиональных умений и опыта профессиональной деятельности Производственная (преддипломная) практика Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты (работа специалиста)

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

Таблица 3.1 – Взаимосвязь планируемых результатов обучения по дисциплине и планируемых результатов освоения образовательной программы

Индекс и содержание компетенции	Знания	Умения	Навыки и (или) опыт деятельности

ПК-3 - способностью проводить анализ защищенности автоматизированных систем	Этап 1: методику анализа защищенности автоматизированных систем	Этап 1: разрабатывать методику анализа защищенности автоматизированных систем	Этап 1: разработки анализа защищенности автоматизированных систем
ПК-3 - способностью проводить анализ защищенности автоматизированных систем	Этап 2: современные стандарты в области информационной безопасности	Этап 2: использовать стандарты в области информационной безопасности	Этап 2: использования стандартов в области информационной безопасности
ПК-8 - способностью разрабатывать и анализировать проектные решения по обеспечению безопасности автоматизированных систем	Этап 1: основные этапы проектирования подсистемы информационной безопасности	Этап 1: разрабатывать основные подсистемы безопасности информации	Этап 1: навыки разработки подсистем информационной безопасности
ПК-8 - способностью разрабатывать и анализировать проектные решения по обеспечению безопасности автоматизированных систем	Этап 2: основные методы технико – экономического обоснования проектных решений	Этап 2: проводить технико – экономическое обоснование проектных решений	Этап 2: навыки технико - экономического обоснования проектных решений
ПК-9 - способностью участвовать в разработке защищенных автоматизированных систем в сфере профессиональной деятельности	Этап 1: основные этапы проектирования подсистемы информационной безопасности	Этап 1: разрабатывать основные подсистемы безопасности информации	Этап 1: навыки разработки подсистем информационной безопасности
ПК-9 - способностью участвовать в разработке защищенных автоматизированных систем в сфере профессиональной деятельности	Этап 2: основные методы технико – экономического обоснования проектных решений	Этап 2: проводить технико – экономическое обоснование проектных решений	Этап 2: навыки технико - экономического обоснования проектных решений
ПК-11 - способностью разрабатывать политику информационной безопасности автоматизированной системы	Этап 1основные составляющие политики безопасности	Этап 1: разрабатывать политику безопасности	Этап 1: навыки разработки политики безопасности
ПК-11 - способностью разрабатывать политику информационной безопасности автоматизированной системы	Этап 2: принципы разработки политики безопасности	Этап 2: применять комплексный подход к обеспечению информационной безопасности	Этап 2: применения комплексного подхода к обеспечению информационной безопасности
ПК-12 - способностью участвовать в	Этап 1: основные этапы проектирова-	Этап 1: разрабатывать основные	Этап 1: навыки разработки подсистем ин-

проектировании системы управления информационной безопасностью автоматизированной системы	ния подсистемы информационной безопасности	подсистемы безопасности информации	формационной безопасности
ПК-12 - способностью участвовать в проектировании системы управления информационной безопасностью автоматизированной системы	Этап 2: основные методы технико – экономического обоснования проектных решений	Этап 2: проводить технико – экономическое обоснование проектных решений	Этап 2: навыки технико - экономического обоснования проектных решений
(ПК-13) - способностью участвовать в проектировании средств защиты информации автоматизированной системы	Этап 1: основные этапы проектирования подсистемы информационной безопасности	Этап 1: разрабатывать основные подсистемы безопасности информации	Этап 1: навыки разработки подсистем информационной безопасности
ПК-13 - способностью участвовать в проектировании средств защиты информации автоматизированной системы	Этап 2: основные методы технико – экономического обоснования проектных решений	Этап 2: проводить технико – экономическое обоснование проектных решений	Этап 2: навыки технико - экономического обоснования проектных решений
ПК-14 - способностью проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации	Этап 1: основные этапы контрольных проверок технических средств защиты информации	Этап 1: разрабатывать методику контрольных проверок технических средств защиты информации	Этап 1: навыки применения контрольных проверок
ПК-14 - способностью проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации	Этап 2: основные принципы работы технических средств защиты информации	Этап 2: разрабатывать способы оценки эффективности применения программных, аппаратных средств защиты информации	Этап 2: навыки оценки эффективности применении аппаратно - программных комплексов
ПК-17 - способностью проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки ин-	Этап 1: методику анализа информационной безопасности	Этап 1: разрабатывать методику анализа информационной безопасности	Этап 1: разработки анализа информационной безопасности

формации			
ПК-17 - способностью проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки информации	Этап 2: современные стандарты в области информационной безопасности	Этап 2: использовать стандарты в области информационной безопасности	Этап 2: использования стандартов в области информационной безопасности
ПК-19 - способностью разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированной системы	Этап 1: основные меры по выполнения обеспечения информационной безопасности	Этап 1: разрабатывать меры по обеспечению информационной безопасности	Этап 1: разработки мер по обеспечению информационной безопасности
ПК-19 - способностью разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированной системы	Этап 2: основные меры поддержки обеспечения информационной безопасности	Этап 2: разрабатывать меры поддержки по обеспечению информационной безопасности	Этап 2: разработки мер поддержки обеспечения информационной безопасности
ПК-21 - способностью разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем	Этап 1: основные этапы оформления рабочей документации	Этап 1: разрабатывать основные рабочие документы	Этап 1: навыки разработки рабочих документов
ПК-21 - способностью разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем	Этап 2: основные нормативные и методические документы	Этап 2: применять нормативные документы в рабочей документации	Этап 2: навыки применения нормативных документов
ПК-22 - способностью участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации	Этап 1основные составляющие политики безопасности	Этап 1: разрабатывать политику безопасности	Этап 1: навыки разработки политики безопасности Этап 2: применения комплексного подхода к обеспечению информационной безопасности

ПК-22 - способностью участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации	Этап 2: принципы разработки политики безопасности	Этап 2: применять комплексный подход к обеспечению информационной безопасности	Этап 2: применения комплексного подхода к обеспечению информационной безопасности
ПК-23 - способностью формировать комплекс мер (правила, процедуры, методы) для защиты информации ограниченного доступа	Этап 1: основные принципы администрирования	Этап 1: проводить процедуру администрирования подсистемы безопасности	Этап 1: навыки администрирования подсистемы безопасности
ПК-23 - способностью формировать комплекс мер (правила, процедуры, методы) для защиты информации ограниченного доступа	Этап 2: современные инструментальные средства администрирования	Этап 2: уметь использовать инструментальные средства администрирования подсистемы безопасности	Этап 2: навыки применения инструментальных средств администрирования подсистемы безопасности
ПК-27 - способностью выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг и аудит безопасности автоматизированной системы	Этап 1: основные меры по выполнения обеспечения информационной безопасности	Этап 1: разрабатывать меры по обеспечению информационной безопасности	Этап 1: разработки мер по обеспечению информационной безопасности
ПК-27 - способностью выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг и аудит безопасности автоматизированной системы	Этап 2: основные меры поддержки обеспечения информационной безопасности	Этап 2: разрабатывать меры поддержки по обеспечению информационной безопасности	Этап 2: разработки мер поддержки обеспечения информационной безопасности

4. Объем дисциплины

Объем дисциплины «Технология защиты информации в различных отраслях деятельности» составляет 5 зачетных единиц (180 академических часов), распределение объема дисциплины на контактную работу обучающихся с преподавателем (КР) и на самостоятельную работу обучающихся (СР) по видам учебных занятий и по периодам обучения представлено в таблице 4.1.

Таблица 4.1 –Распределение объема дисциплины по видам учебных занятий и по периодам обучения, академические часы

№ п/п	Вид учебных занятий	Итого КР	Итого СР	Семестр № 7		Семестр № 8	
				КР	СР	КР	СР
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**
1	Лекции (Л)	52		34		18	
2	Лабораторные работы (ЛР)						
3	Практические занятия (ПЗ)	50		32		18	
4	Семинары(С)						
5	Курсовое проектирование (КП)						
6	Рефераты (Р)						
7	Эссе (Э)						
8	Индивидуальные домашние задания (ИДЗ)						
9	Самостоятельное изучение вопросов (СИВ)				20		16
10	Подготовка к занятиям (ПкЗ)				20		16
11	Промежуточная аттестация	6		2		4	
12	Наименование вида промежуточной аттестации	х	х	зачёт		экзамен	
13	Всего	108	72	68	40	40	32

5. Структура и содержание дисциплины

Структура дисциплины представлена в таблице 5.1.

Таблица 5.1. Структура дисциплины

№ п/п	Наименования разделов и тем	Семестр	Объем работы по видам учебных занятий, академические часы										Коды формируемых компетенций
			лекции	лабораторная работа	практические занятия	семинары	курсовое проектирование	рефераты (эссе)	индивидуальные домашние задания	самостоятельное изучение вопросов	подготовка к занятиям	промежуточная аттестация	
1	2	3	4	5	6	7	8	9	10	11	12	13	14
1.	**Раздел 1 Введение. Предмет дисциплины. Моделирование систем обеспечения информационной безопасности**	**7**	**12**		**10**			**x**		**4**	**4**	**x**	**ПК-3; ПК-8; ПК-9;**
1.1.	**Тема 1** Определение понятия «информация», ее существенные признаки	**7**	6		6			**x**		2	2	**x**	ПК-3; ПК-8; ПК-9;
1.2.	**Тема 2** Системный подход к построению систем обеспечения информационной безопасности	**7**	6		4			**x**		2	2	**x**	ПК-3; ПК-8; ПК-9;
2.	**Раздел 2 Законодательное регулирование и стандартизация**	**7**	**10**		**10**			**x**		**4**	**4**	**x**	**ПК-11; ПК-12; ПК-13;**
2.1.	**Тема 3** Структура органов государственной власти РФ	**7**	6		6			**x**		2	2	**x**	ПК-11; ПК-12; ПК-13;
2.2.	**Тема 4** Роль стандартизации в регулировании области обеспечения ИБ	**7**	4		4			**x**		2	2	**x**	ПК-11; ПК-12; ПК-13;
3.	**Раздел 3 Дополнительные аспекты работы стека протоколов TCP/IP**	**7**	**6**		**6**			**x**		**6**	**6**	**x**	**ПК-11; ПК-12; ПК-13;**

№ п/п	Наименования разделов и тем	Семестр	Объем работы по видам учебных занятий, академические часы										Коды формируемых компетенций
			лекции	лабораторная работа	практические занятия	семинары	курсовое проектирование	рефераты (эссе)	индивидуальные домашние задания	самостоятельное изучение вопросов	подготовка к занятиям	промежуточная аттестация	
1	2	3	4	5	6	7	8	9	10	11	12	13	14
3.1	**Тема 5** Сравнение модели стека протоколов TCP/IP с моделью OSI	**7**	2		2			**x**		2	2	**x**	ПК-11; ПК-12; ПК-13;
3.2	**Тема 6** Флаги TCP-пакета	**7**	4		4			**x**		4	4	**x**	ПК-11; ПК-12; ПК-13;
4	**Раздел 4 Основные алгоритмы шифрования, используемые для защиты информации в компьютерных сетях**	**7**	**6**		**6**			**x**		**6**	**6**	**x**	**ПК-11; ПК-12; ПК-13;**
4.1	**Тема 7** Проблемы и задачи, разрешаемые криптографическими методами	**7**	4		4			**x**		4	4	**x**	ПК-11; ПК-12; ПК-13;
4.2	**Тема 8** DES и его модификации	**7**	2		2			**x**		2	2	**x**	ПК-11; ПК-12; ПК-13;
5.	**Контактная работа**	**7**	**34**		**32**			**x**				**2**	**x**
6.	**Самостоятельная работа**	**7**								**20**	**20**		**x**
7.	**Объем дисциплины в семестре**	**7**	**34**		**32**					**20**	**20**	**2**	**x**
8	**Раздел 5 Введение в IPSec**	**8**	**2**		**2**			**x**		**4**	**4**	**x**	**ПК-14; ПК-17; ПК-19;**
8.1	**Тема 9** Основные протоколы IPSec	**8**	2		2			**x**		4	4	**x**	ПК-14; ПК-17; ПК-19;
9	**Раздел 6 Усиление безопасности ОС Microsoft Windows**	**8**	**6**		**6**			**x**		**4**	**4**	**x**	**ПК-14; ПК-17; ПК-19;**

№ п/п	Наименования разделов и тем	Семестр	Объем работы по видам учебных занятий, академические часы										Коды формируемых компетенций
			лекции	лабораторная работа	практические занятия	семинары	курсовое проектирование	рефераты (эссе)	индивидуальные домашние задания	самостоятельное изучение вопросов	подготовка к занятиям	промежуточная аттестация	
1	2	3	4	5	6	7	8	9	10	11	12	13	14
9.1	**Тема 10** Схема реализации систем безопасности в ОС Windows Server	**8**	2		2			**x**		2	2	**x**	ПК-14; ПК-17; ПК-19;
9.2	**Тема 11** Встроенные средства безопасности NTFS	**8**	4		4			**x**		2	2	**x**	ПК-14; ПК-17; ПК-19;
10	**Раздел 7 Техника сетевых атак и механизмы защиты**	**8**	**6**		**6**			**x**		**6**	**6**	**x**	**ПК-14; ПК-17; ПК-19;**
10.1	**Тема 12** Классификация нарушителей в зависимости от целей и мотивов атак	**8**	2		2			**x**		2	2	**x**	ПК-14; ПК-17; ПК-19;
10.2	**Тема 13** Утилиты удаленного администрирования	**8**	4		4			**x**		4	4	**x**	ПК-21; ПК-22; ПК-23; ПК-27
11	**Раздел 7 Получение неавторизованного доступа к операционной**	**8**	**4**		**4**			**x**		**2**	**2**	**x**	**ПК-21; ПК-22; ПК-23; ПК-27**
11.1	**Тема 14** Уязвимости ОС при наличии неограниченного физического доступа к аппаратной платформе	**8**	4		4			**x**		2	2	**x**	ПК-21; ПК-22; ПК-23; ПК-27
12	**Контактная работа**	**8**	**18**		**18**			**x**				**4**	**x**
13	**Самостоятельная работа**	**8**						**x**		**16**	**16**		**x**
14	**Объем дисциплины в семестре**	**8**	**18**		**18**					**16**	**16**	**4**	**x**
15	**Всего по дисциплине**	**x**	**52**		**50**					**36**	**36**	**6**	**x**

5.2. Содержание дисциплины

5.2.1 – Темы лекций

№ п.п.	Наименование темы лекции	Объем, академические часы
7 семестр		34
Л-1-2	Введение. Предмет дисциплины	4
Л-3-4	Моделирование систем обеспечения информационной безопасности	4
Л-5-6	Структура органов государственной власти РФ.	4
Л-7-8	Роль стандартизации в регулировании области обеспечения ИБ	4
Л-9	Сравнение модели стека протоколов TCP/IP с моделью OSI.	2
Л-10	Назначение RFC	2
Л-11	Флаги TCP-пакета	2
Л-12	Структура заголовка пакетов протоколов IP, ICMP, TCP, UDP	2
Л-13	Принципы работы FTP-сервиса. Активный и пассивный режим FTP-сервера	2
Л-14	Типы соединений RFC	2
Л-15-16	Симметричные алгоритмы, принцип работы. Сеть Фейштеля	4
Л-17	Цифровые сертификаты. Стандарт X.509. Архитектура PKI	2
8 семестр		18
Л-18	Цели и задачи расширения безопасности IP протокола	2
Л-19	База Данных Политики Безопасности (SPD)	2
Л-20	Основные протоколы IPSec: Authentication Header (AH) и Encapsulating Security Payload (ESP). Уровень реализации IPSec	2
Л-21	Принципы построения Active Directory. Основные элементы дерева на логическом и физическом уровнях	2
Л-22	Организация сетевого доступа к папкам. Виды разграничения доступа. Комбинация прав доступа к сетевым файловым ресурсам и доступа к объектам NTFS	2
Л-23	PDCA-модель. Роль процесса контроля	2
Л-24	Классификация нарушителей в зависимости от целей и мотивов атак	2
Л-25	Атаки, основанные на уязвимостях: получение контроля, DoS-атаки. Сокрытие следов атаки	2
Л-26	Утилиты удаленного администрирования (консольный доступ): текстовая и графическая консоли	2
Итого по дисциплине		52

5.2.2 – Темы практических занятий

№ п.п.	Наименование темы практического занятия	Объем, академические часы
7 семестр		32
ПЗ-1-5	Microsoft Virtual PC	10
ПЗ-6-10	Оценка профилей защиты и заданий по безопасности	10
ПЗ-11-16	Использование утилиты PGP для генерации ключей и обмена шифрованной информацией	12
8 семестр		18
ПЗ-17	Настройка защищенного соединения средствами IPSec	2
ПЗ-18	Анализ трафика, генерируемого протоколами AH, ESP	2
ПЗ-19	Настройка локального механизма шифрования в Windows Server на базе EFS	2
ПЗ-20	Ограничение доступа к разделам реестра, утилитам по работе с реестром. Экспорт и импорт данных реестра. Удаленный доступ к реестру	2
ПЗ-21	Использование утилиты консольного управления UltraVNC	2
ПЗ-22-23	Удаленное управление рабочей станцией с помощью средств «троянского коня» NetBus Pro	4
ПЗ-24-25	Сканирование IP-подсетей с помощью утилит SuperScan4, NetScan Tools Pro 2001, XSpaider	4
Итого по дисциплине		50

5.2.3 – Вопросы для самостоятельного изучения

№ п.п.	Наименования темы	Наименование вопроса	Объем, академические часы
1.	Определение понятия «информция, ее существенные признаки	Определение понятия информация, ее существенные признаки. Основные виды информации.	2
2.	Системный подход к построению систем обеспечения информационной безопасности	Системный подход к построению систем обеспечения информационной безопасности. Составляющие модели ИБ: основы, направления, этапы. Сводная матрица задач реализации модели ИБ. Угрозы, их классификация: объективные (естественные) и субъективные (непреднамеренные и преднамеренные).	2

3.	Структура органов государственной власти РФ	Информационное право: предмет и методы отрасли. Нормативно-правовое обеспечение защиты информации: законы, федеральные и локальные нормативные акты.	2
4.	Роль стандартизации в регулировании в области обеспечения ИБ	Серия стандартов ISO/IEC (ИСО/МЭК) 27000. Стандарты ИТ: ITIL, ISO/IEC 20000. Оценка безопасности: стандарты ISO/IEC 15408, CobIT Политика РФ в области лицензирования и технического регулирования	2
5.	Сравнение модели стека протоколов TCP/IP с моделью OSI	Общие понятия. Протокол. Стек протоколов. Протоколы взаимодействия приложений и протоколы транспортной подсистемы. Стек протоколов TCP/IP Сетевая модель OSI	2
6.	Флаги TCP-пакета	Трехступенчатая процедура установления соединения в протоколе TCP Процедуры разрыва TCP-соединения	4
7.	Проблемы и задачи, разрешаемые криптографическими методами	Основные алгоритмы шифрования, используемые для защиты информации в компьютерных сетях.	4
8.	DES и его модификации	Виды атак: Атака Винера на RSA, атаки на RSA основанные на решетках, атака Хостада, атака Франклина-Рейтера, частичное раскрытие ключа. Стойкость актуальных алгоритмов шифрования. Доказуемая стойкость со случайным оракулом. Доказуемая стойкость без случайного оракула	2
9.	Основные протоколы IPSec	Прозрачность IPSec для ко-	2

		нечных пользователей и приложений. Защита от изменения данных. Глубокая защита протоколов и приложений верхнего уровня. Основные протоколы IPSec: Authentication Header (AH) и Encapsulating Security Payload (ESP). Уровень реализации IPSec	
10.	Схема реализации систем безопасности в ОС Windows Server	Настройка шифрования в Windows Server. Навык шифрования в Windows Server.	4
11.	Встроенные средства безопасности NTFS	Виды разграничения доступа. Комбинация прав доступа к сетевым файловым ресурсам и доступа к объектам NTFS. Организация сетевого доступа к папкам. Виды разграничения доступа. Комбинация прав доступа к сетевым файловым ресурсам и доступа к объектам NTFS	2
12.	Классификация нарушителей в зависимости от целей и мотивов атак	Классификация нарушителей в зависимости от целей и мотивов атак	2
13.	Утилиты удаленного администрирования	Утилиты удаленного администрирования (консольный доступ): текстовая и графическая консоли	4
14.	Уязвимости ОС при наличии неограниченного физического доступа к аппаратной платформе	Уязвимости ОС при наличии неограниченного физического доступа к аппаратной платформе	2

6. Учебно-методическое и информационное обеспечение дисциплины

6.1 Основная литература, необходимая для освоения дисциплины

1. Аверченков В.И. Служба защиты информации. Организация и управление [Электронный ресурс]: учебное пособие для вузов/ Аверченков В.И., Рытов М.Ю.— Электрон. текстовые данные.— Брянск: Брянский государственный технический университет, 2012.— 186 с.

2. Разработка системы технической защиты информации [Электронный ресурс]: учебное пособие/ В.И. Аверченков [и др.].— Электрон. текстовые данные.— Брянск: Брянский государственный технический университет, 2012.— 187 c.

6.2 Дополнительная литература, необходимая для освоения дисциплины

1. Лапонина О.Р. Основы сетевой безопасности: криптографические алгоритмы и протоколы взаимодействия: курс лекций: учебное пособие. Издательство: Интернет-Университет Информационных Технологий, 2009 г.- 608 с.

2. Авдошин С.М., Сердюк В.А., Савельева А.А. Технологии и продукты Microsoft в обеспечении информационной безопасности. Издательство: Интернет-Университет Информационных Технологий, 2010 г.- 455 с

3. Сидельников В.М. Теория кодирования. Издательство: ФИЗМАТЛИТ, 2011 г.- 323 с.

6.3 Методические материалы для обучающихся по освоению дисциплины и другие материалы к занятиям

Электронное учебное пособие, включающее:

- конспект лекций;
- методические материалы по выполнению практических (семинарских) работ.

6.4 Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

Электронное учебное пособие, включающее:

- методические рекомендации по самостоятельному изучению вопросов;
- методические рекомендации по подготовке к занятиям.

6.5 Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем

1. дистрибутив Windows 2003 Server;
2. Service Pack 3 для Windows 2003 Server;
3. образ загрузочного диска ERD Commander 2002;
4. PGP;
5. SuperScan; NetScan Tools Pro 2001; XSpaider;
6. UltraVNC;
7. NetBus Pro;
8. Snadboy Revelation v 2;
9. L0phtCrack v3.02;
10. KeyLogger.

7. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

Занятия лекционного типа проводятся в аудитории, оборудованной мультимедиа проектором, компьютером, учебной доской.

Таблица 7.1 – Материально-техническое обеспечение лабораторных занятий

Вид и номер занятия	Тема занятия	Название аудитории	Название оборудования	Название технических и электронных средств обучения и контроля знаний
1	2	3	4	5
7 семестр				
ПЗ-1-5	Microsoft Virtual PC	943 «Лаборатория технологий, методов программирования и программного обеспечения»	Персональный ПК с установленным специальным ПО	SuperScan; NetScan Tools Pro 2001; XSpaider; UltraVNC; NetBus Pro;
ПЗ-6-10	Оценка профилей защиты и заданий по безопасности	943 «Лаборатория технологий, методов программирования и программного обеспечения»	Персональный ПК с установленным специальным ПО	SuperScan; NetScan Tools Pro 2001; XSpaider; UltraVNC; NetBus Pro;
ПЗ-11-16	Использование утилиты PGP для генерации ключей и обмена шифрованной информацией	943 «Лаборатория технологий, методов программирования и программного обеспечения»	Персональный ПК с установленным специальным ПО	SuperScan; NetScan Tools Pro 2001; XSpaider; UltraVNC; NetBus Pro;
8 семестр				
ПЗ-1	Настройка защищенного соединения средствами IPSec	943 «Лаборатория технологий, методов программирования и программного обеспечения»	Персональный ПК с установленным специальным ПО	SuperScan; NetScan Tools Pro 2001; XSpaider; UltraVNC; NetBus Pro;
ПЗ-2	Анализ трафика, генерируемого протоколами AH, ESP	943 «Лаборатория технологий, методов программирования и программного обеспечения»	Персональный ПК с установленным специальным ПО	SuperScan; NetScan Tools Pro 2001; XSpaider; UltraVNC; NetBus Pro;
ПЗ-3	Настройка локального механизма шифрования в	943 «Лаборатория технологий, методов программиро-	Персональный ПК с установленным специ-	SuperScan; NetScan Tools Pro 2001;

	Windows Server на базе EFS	вания и программного обеспечения»	альным ПО	XSpaider; UltraVNC; NetBus Pro;
ПЗ-4	Ограничение доступа к разделам реестра, утилитам по работе с реестром. Экспорт и импорт данных реестра. Удаленный доступ к реестру	943 «Лаборатория технологий, методов программирования и программного обеспечения»	Персональный ПК с установленным специальным ПО	SuperScan; NetScan Tools Pro 2001; XSpaider; UltraVNC; NetBus Pro;
ПЗ-5	Использование утилиты консольного управления UltraVNC	943 «Лаборатория технологий, методов программирования и программного обеспечения»	Персональный ПК с установленным специальным ПО	SuperScan; NetScan Tools Pro 2001; XSpaider; UltraVNC; NetBus Pro;
ПЗ-6	Удаленное управление рабочей станцией с помощью средств «троянского коня» NetBus Pro	943 «Лаборатория технологий, методов программирования и программного обеспечения»	Персональный ПК с установленным специальным ПО	SuperScan; NetScan Tools Pro 2001; XSpaider; UltraVNC; NetBus Pro;
ПЗ-7	Сканирование IP-подсетей с помощью утилит SuperScan4, NetScan Tools Pro 2001, XSpaider	943 «Лаборатория технологий, методов программирования и программного обеспечения»	Персональный ПК с установленным специальным ПО	SuperScan; NetScan Tools Pro 2001; XSpaider; UltraVNC; NetBus Pro;
ПЗ-8	Использование утилиты перехвата клавиатурного ввода – KeyLogger	943 «Лаборатория технологий, методов программирования и программного обеспечения»	Персональный ПК с установленным специальным ПО	SuperScan; NetScan Tools Pro 2001; XSpaider; UltraVNC; NetBus Pro;
ПЗ-9	Использование возможности «сброса» паролей служебных учетных записей Windows Server/WorkStation при неограниченном физическом доступе	943 «Лаборатория технологий, методов программирования и программного обеспечения»	Персональный ПК с установленным специальным ПО	SuperScan; NetScan Tools Pro 2001; XSpaider; UltraVNC; NetBus Pro;

Занятия лекционного типа проводятся в учебной аудитории для проведения занятий лекционного типа с набором демонстрационного оборудования, обеспечивающие тематические иллюстрации, укомплектованной специализированной мебелью и техническими средствами обучения.

Занятия семинарского типа проводятся в учебных аудиториях для проведения занятий семинарского типа, укомплектованных специализированной мебелью и техническими средствами обучения.

Консультации по дисциплине проводятся в учебных аудиториях для групповых и индивидуальных консультаций, укомплектованных специализированной мебелью и техническими средствами обучения.

Текущий контроль и промежуточная аттестация проводится в учебных аудиториях для текущего контроля и промежуточной аттестации, укомплектованных специализированной мебелью и техническими средствами обучения.

Самостоятельная работа студентов проводится в помещениях для самостоятельной работы, укомплектованном специализированной мебелью и техническими средствами обучения. Учебное оборудование хранится и обслуживается в помещениях для хранения и профилактического обслуживания учебного оборудования.

Оценочные материалы для проведения текущего контроля и промежуточной аттестации обучающихся по дисциплине представлены в Приложении 6.

Программа разработана в соответствии с ФГОС ВО по направлению подготовки 10.05.03 Информационная безопасность автоматизированных систем, утвержденным приказом Министерства образования и науки РФ № 1509 от 01.12.2016

Разработал(и): _____ Урбан В.А.