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

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.Б.18 Техническая защита информации

Направление подготовки 10.03.01 Информационная безопасность

Профиль подготовки Безопасность автоматизированных систем

Квалификация (степень) выпускника бакалавр

Форма обучения очная

1. **Цели освоения дисциплины:**

- раскрыть основы правового регулирования отношений в информационной сфере, конституционные гарантии прав граждан на получение информации и механизм их реализации, понятия и виды защищаемой информации по законодательству РФ, систему защиты государственной тайны, основы правового регулирования отношений в области интеллектуальной собственности и способы защиты этой собственности, понятие и виды компьютерных преступлений, а также приобретение студентами знаний по организационному обеспечению защиты информации и формирование основных практических навыков работы в данной области.

2. Место дисциплины в структуре ООП

Дисциплина «Техническая защита информации» к базовой части. Требования к предшествующим знаниям представлены в таблице 2.1. Перечень дисциплин, для которых дисциплина «Техническая защита информации» является основополагающей, представлен в таблице 2.2.

Таблица 2.1. Требования к пререквизитам дисциплины

Компетенция	Дисциплина
ОК-5	Социология Основы информационной безопасности
ПК-4	Безопасность вычислительных сетей
ПК-4	Технология построения защищенных автоматизированных систем
ПК-4	Производственная эксплуатационная практика
ПК-6	Метрология, стандартизация и сертификация
ПК-6	Производственная эксплуатационная практика
ПК-11	Теория вероятностей и математическая статистика
ПК-11	Основы научных исследований
ПК-11	Математическая статистика
ПК-12	Моделирование систем
ПК-12	Основы научных исследований
ПК-12	Математическая статистика
ПК-12	3D-моделирование

Таблица 2.2. Требования к постреквизитам дисциплины

Компетенция	Дисциплина
ОК-5	Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты (работа бакалавра)
ПК-4	Производственная (преддипломная) практика
ПК-6	Производственная (преддипломная) практика
ПК-11	Производственная (преддипломная) практика
ПК-12	Производственная (преддипломная) практика
ПК-4	Защита выпускной квалификационной работы, включая подготовку к процедуре

	защиты и процедуру защиты (работа бакалавра)
ПК-6	Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты (работа бакалавра)
ПК-11	Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты (работа бакалавра)
ПК-12	Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты (работа бакалавра)

3. Компетенции обучающегося, формируемые в результате освоения дисциплины

3.1. Компетенции, формируемые в результате освоения дисциплины:

В результате изучения дисциплины «Техническая защита информации» студент должен владеть:

Индекс и содержание компетенции	Знания	Умения	Навыки и (или) опыт деятельности
ОК-5 способностью понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики	Этап 1 Цели, задачи, принципы и основные направления обеспечения технической защиты информации государства.	Этап 1 Проводить анализ и давать оценку степени защищенности компьютерных систем, осуществлять повышение уровня технических средств защиты информации	Этап 1 Профессиональной терминологией и методами теоретического обоснования в выборе технических средств обеспечения информационной безопасности
ОК-5 способностью понимать социальную	Этап 2 Современные подходы к обеспечению систем	Этап 2 Применять отечественные и зарубежные стандарты в области	Этап 2 Владеть методологическим и принципами оценки

значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики	технической защиты информации и интересов личности, общества и государства	обеспечения технической защиты информации, интересов личности, общества и государства	технической защиты информации и защиты интересов личности, общества и государства
ПК-4 - способностью участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты	Этап 1 Основные правила разработки политики безопасности организации. Компоненты политики безопасности	Этап 1 Умения разработки политики безопасности организации, согласно правовыми нормативными актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службой по техническому и экспортному контролю;	Этап 1 Внедрения политики безопасности в организации, согласно правовыми нормативными актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службой по техническому и экспортному контролю; согласно правовыми нормативными актами и нормативными методическими документами Федеральной службы безопасности Российской

			Федерации, Федеральной службой по техническому и экспортному контролю
ПК-4 - способностью участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты	Этап 2 Принципы и методы противодействия несанкционированному информационному воздействию на технические обьекты	Этап 2 Осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты.	Этап 2 Навыки применения комплексного подхода к обеспечению информационной безопасности объекта защиты
ПК-6 - Способностью принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и техническихсредств защиты информации	Этап 1 Знание основных программно-аппаратных средств защиты информации	Этап 1 Умения настройки основных программно-аппаратных средств защиты информации	Этап 1 Навыки организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных
	Этап 2 Знание основных технических средств защиты информации	Этап 2 Умения работы с основными техническими средствами защиты информации	Этап 2 Навыки организации и проведении контрольных проверок работоспособности и эффективности применяемых технических средств защиты информации
ПК-11 - способностью проводить	Этап 1 Основные понятия и методы теории	Этап 1 Умения проведения эксперимента в	Этап 1 Навыки использовать

эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов	вероятностей и математической статистики;	системах защиты информации	математические методы и модели для решения прикладных задач.
	Этап 2 Математические методы обработки экспериментальных данных.	Этап 2 Умения обработки оценки погрешности и достоверности их результатов	Этап 2 Навыки обработки, оценки погрешности и достоверности их результатов
ПК-12 - Способностью принимать участие в проведении экспериментальных исследований системы защиты информации	Этап 1 Основные понятия и методы теории вероятностей и математической статистики;	Этап 1 Умения проведения эксперимента в системах защиты информации	Этап 1 Навыки принимать участие в проведении экспериментальных исследований системы защиты информации
ПК-12 - Способностью принимать участие в проведении экспериментальных исследований системы защиты информации	Этап 2 Математические методы обработки экспериментальных данных.	Этап 2 Умения обработки результатов экспериментальных исследований системы защиты информации	Этап 2 Навыки формирования отчетности по результатам проведения экспериментальных исследований системы защиты информации

4. Объем дисциплины

Объем дисциплины «Техническая защита информации» составляет 4 зачетные единицы (144 академических часа), 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 № 8	
				КР	СР

1	2	3	4	5	6
1	Лекции (Л)	26		26	
2	Лабораторные работы (ЛР)	12		12	
3	Практические занятия (ПЗ)	26		26	
4	Семинары(С)				
5	Курсовое проектирование (КП)				
6	Рефераты (Р)				
7	Эссе (Э)				
8	Индивидуальные домашние задания (ИДЗ)				
9	Самостоятельное изучение вопросов (СИВ)		32		32
10	Подготовка к занятиям (ПкЗ)		44		44
11	Промежуточная аттестация	4		4	
12	Наименование вида промежуточной аттестации	х	х	экзамен	
13	Всего	68	76	68	76

5. Структура и содержание дисциплины

Структура дисциплины представлена в таблице 5.1.

Таблица 5.1. Структура дисциплины

№ п/п	Наименованияразделов 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 Основные понятия и определения.**	**8**	**8**	**4**	**8**			**x**		**8**	**11**	**x**	ОК-5 ПК-4; ПК-6; ПК-11; ПК-12
1.1.	Тема 1 Термины и определения в области технической защиты информации.	**8**	4	2	4			**x**		4	5	**x**	ОК-5 ПК-4; ПК-6; ПК-11; ПК-12
1.2.	Тема 2 Классификация технических каналов утечки информации.	**8**	4	2	4			**x**		4	6	**x**	ПК-4; ПК-6; ПК-11; ПК-12
2.	**Раздел 2 Технические каналы утечки информации, обрабатываемой средствами**	**8**	**6**	**4**	**6**			**x**		**8**	**11**	**x**	ОК-5 ПК-4; ПК-6; ПК-11; ПК-12

№ п/п	Наименованияразделов 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
	вычислительной техники и автоматизированными системами.												
2.1.	Тема 3 Общая характеристика и классификация технических каналов утечки информации, обрабатываемой средствами вычислительной техники и автоматизированными системами.	**8**	4	2	4			**х**		4	5	**х**	ПК-4; ПК-6; ПК-11; ПК-12
2.2.	Тема 4 Виды каналов утечки информации	**8**	2	2	2			**х**		4	6	**х**	ОК-5 ПК-4; ПК-6; ПК-11; ПК-12
3	**Раздел 3** **Системный подход к инженерно-технической защите информации.**	**8**	6	2	6			**х**		8	11	**х**	ПК-4; ПК-6; ПК-11; ПК-12
3.1	Тема 5 Способы и средства защиты информации,	**8**	2	2	2			**х**		4	5		ОК-5 ПК-4; ПК-6;

№ п/п	Наименованияразделов 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
	обрабатываемой средствами вычислительной техники и автоматизированными системами.												ПК-11; ПК-12
3.2	Тема 6 Способы и средства защиты выделенных помещений от утечки речевой информации по техническим каналам.	**8**	4		4			**x**		4	6		ОК-5 ПК-4; ПК-6; ПК-11; ПК-12
4	**Раздел 4 Основные этапы проектирования системы защиты информации техническими средствами.**	**8**	6	2	6			**x**		8	11		ПК-4; ПК-6; ПК-11; ПК-12
4.1	Тема 7 Организация технической защиты информации.	**8**	2	2	2			**x**		4	5		ОК-5 ПК-4; ПК-6; ПК-11; ПК-12
4.2	Тема 8 Лицензирование деятельности по	**8**	4		4			**x**		4	6		ПК-4; ПК-6; ПК-11;

№ п/п	Наименованияразделов 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
	технической защите информации.												ПК-12
3.	**Контактная работа**	**8**	**26**	**12**	**26**			**x**				**4**	**x**
4.	**Самостоятельная работа**	**8**						**x**		**32**	**44**		**x**
5.	**Объем дисциплины в семестре**	**8**	**26**	**12**	**26**							**4**	**x**
6.	**Всего по дисциплине**	**x**	**26**	**12**	**26**					**32**	**44**	**4**	**x**

5.2. Содержание дисциплины

5.2.1 – Темы лекций

№ п.п.	Наименование темы лекции	Объем, академические часы
Л-1	Термины и определения в области технической защиты информации.	2
Л-2	Классификация технических каналов утечки информации.	2
Л-3	Общая характеристика и классификация технических каналов утечки информации, обрабатываемой средствами вычислительной техники и автоматизированными системами.	2
Л-4	Акустические (речевые) и оптические каналы утечки информации	2
Л-5	Радиоэлектронные каналы утечки информации	2
Л-6	Материально-вещественные каналы утечки информации.	2
Л-7	Способы и средства защиты информации, обрабатываемой средствами вычислительной техники и автоматизированными системами.	2
Л-8	Способы и средства защиты выделенных помещений от утечки речевой информации по техническим каналам.	2
Л-9	Методы и средства контроля эффективности технической защиты информации, обрабатываемой средствами вычислительной техники и автоматизированными системами	2
Л-10	Методы и средства контроля эффективности защиты выделенных помещений от утечки речевой информации по техническим каналам	2
Л-11	Требования к средствам измерения побочных электромагнитных излучений и наводок средств вычислительной техники и условиям проведения измерений.	2
Л-12	Организация технической защиты информации.	2
Л-13	Лицензирование деятельности по технической защите информации	2
Итого по дисциплине		26

5.2.2 – Темы лабораторных работ

№ п.п.	Наименование темы лекции	Объем, академические часы
ЛР-1	Побочные электромагнитные излучения средств вычислительной техники	4
ЛР-2	Электромагнитные наводки от средств вычислительной техники в линейных коммуникациях	2
ЛР-3	Пассивные и активные методы защиты от наводки	2

	средств вычислительной техники в линейных коммуникациях	
ЛР-4	Оценка защищенности выделенного помещения от утечки информации по акустическому и виброакустическому каналам	2
ЛР-5	Изучение средств обеспечения конфиденциальности данных	2
Итого по дисциплине		12

5.2.3 Темы практических занятий

№ п.п.	Наименование темы лекции	Объем, академические часы
ПЗ-1	Стандарты в области технической защиты информации.	12
ПЗ -2	Защита от побочных электромагнитных излучений средств вычислительной техники пространственным зашумлением	2
ПЗ -3	Стандарты в области технической защиты информации.	12
Итого по дисциплине		26

5.2.4 – Вопросы для самостоятельного изучения

№ п.п.	Наименования темы	Наименование вопроса	Объем, академические часы
1.	Термины и определения в области технической защиты информации	Нормативные документы по технической защите информации.	4
2.	Классификация технических каналов утечки информации	Виды технических каналов утечки информации.	4
3.	Общая характеристика, и классификация технических каналов утечки информации, обрабатываемойсредствами вычислительной техники и автоматизированными системами	Технический канал утечки информациисоздаваемый путем внедрения в СВТ электронных устройств негласного получения информации.	4
4.	Виды каналов утечки информации	Средства акустической разведки и их технические характеристики.	4
5.	Способы и средства защиты информации,обрабатываемойсредствами вычислительной техники и автоматизированными	Специальные технические средства подавления электронных устройств перехвата речевой информации	4

	системами	(широкополосные генераторы шума, блокираторы средств сотовой связи, активные средства защиты телефонных линий связи).	
6.	Способы и средства зашиты выделенных помещений от утечки речевой информации по техническим каналам	Методика контроля эффективности защиты выделенных помещений при использовании систем виброакустической маскировки.	4
7.	Организация технической защиты информации	Порядок ввода объекта информатизации и системы технической защиты информации в эксплуатацию.	4
8.	Лицензирование деятельности по технической защите информации	Порядок лицензирования деятельности по технической защите конфиденциальной информации	4
Итого по дисциплине			32

6. Учебно-методическое и информационное обеспечение дисциплины

6.1 Основная литература, необходимая для освоения дисциплины

1. Галатенко. В.А. Основы информационной безопасности [электронный ресурс]: курс лекций: учебное пособие / под ред. В.Б. Бетелина. Издательство: Интернет-Университет Информационных Технологий. 2007. - 208 с.
2. Галатенко. В.А. Стандарты информационной безопасности: курс лекций: учебное пособие. Издательство Основы информационной безопасности [электронный ресурс]: Интернет-Университет Информационных Технологий, 2007 264 с.

6.2 Дополнительная литература, необходимая для освоения дисциплины

1. Попов, В.Б. Основы информационных и телекоммуникационных технологий. Основы информационной безопасности Основы информационной безопасности [электронный ресурс]: Учебное пособие Издательство: Финансы и статистика, 2007. - 174 с.
2. Лапонина. О.Р. Межсетевое экранирование Основы информационной безопасности [электронный ресурс]: Учебное пособие. Издательство: Интернет-Университет Информационных Технологий: БИНОМ. Лаборатория знаний, 2007 - 344 с.

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

Электронное учебное пособие, включающее:
- конспект лекций;
- методические указания по выполнению лабораторных работ;
- методические указания 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

7. 1. Open Office
8. 2. JoliTest (JTRun, JTEditor, TestRun)
9. **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

Номер работы	Тема лабораторной работы	Название специализированной лаборатории	Название спецоборудования	Название технических и электронных средств обучения и контроля знаний
ЛР-1	Побочные электромагнитные излучения средств вычислительной техники	941, 943 аудитории ИУР и КБ	персональный компьютер	Специализированные программные и технические средства
ЛР -2	Электромагнитные наводки от средств вычислительной техники в линейных коммуникациях	941, 943 аудитории ИУР и КБ	персональный компьютер	Специализированные программные и технические средства
ЛР -3	Пассивные и активные методы защиты от наводки средств вычислительной техники в линейных коммуникациях	941, 943 аудитории ИУР и КБ	персональный компьютер	Специализированные программные и технические средства
ЛР -4	Оценка защищенности выделенного помещения от утечки информации по акустическому и виброакустическому каналам.	941, 943 аудитории ИУР и КБ	персональный компьютер	Специализированные программные и технические средства
ЛР -5	Изучение средств	941, 943 аудитории	персональный	Специализированные

	обеспечения конфиденциальности данных	ИУР и КБ	компьютер	программные и технические средства

Таблица 7.2 Материально-техническое обеспечение практических занятий

Номер работы	Тема практического занятия	Название специализированной лаборатории	Название спецоборудования	Название технических и электронных средств обучения и контроля знаний
ПЗ-1	Стандарты в области технической защиты информации.	941, 943 аудитории ИУР и КБ	персональный компьютер	Microsoft Office Word, Microsoft Power Point
ПЗ-2	Защита от побочных электромагнитных излучений средств вычислительной техники пространственным зашумлением	941, 943 аудитории ИУР и КБ	персональный компьютер	Microsoft Office Word, Microsoft Power Point
ПЗ-3	Стандарты в области технической защиты информации.	941, 943 аудитории ИУР и КБ	персональный компьютер	Microsoft Office Word, Microsoft Power Point

Лабораторные занятия проводятся в специальных аудиториях, оборудованных учебными приборами, учебной доской, рабочим местом преподавателя (стол, стул), а также посадочными местами для обучающихся, число которых соответствует численности обучающихся в группе (таблица 7.1).

Занятия семинарского типа (практические занятия) проводятся в аудиториях, оборудованных учебной доской, рабочим местом преподавателя (стол, стул), а также посадочными местами для обучающихся, число которых соответствует численности обучающихся в группе.

Оценочный материал для проведения промежуточной аттестации обучающихся по дисциплине представлен в Приложении 6.

Программа разработана в соответствии с Федеральным государственным образовательным стандартом высшего образования по направлению подготовки 10.03.01 Информационная безопасность, утвержденным приказом Министерства образования и науки РФ № 1515 от 01.12.2016 г.

Разработал(и): _____ Полищук Ю.В.