

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

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1. Б.2. 06 Инженерно-техническая защита информации и технические средства на критически важных объектах

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:

- ознакомление с основными источниками и носителями информации различных видов;
- изучение демаскирующих признаков объектов защиты;
- ознакомление с угрозами безопасности информации;
- изучение принципов добывания информации;
- ознакомление с техническими каналами утечки информации, обрабатываемой средствами вычислительной техники и автоматизированными системами;
- изучение способов и средств защиты информации, обрабатываемой техническими средствами;
- изучение способов и средств защиты информации от наблюдения;
- изучение способов и средств защиты выделенной информации от перехвата;
- изучение способов и средств защиты выделенных (защищаемых) помещений от утечки акустической (речевой) информации;
- изучение методов и средств контроля эффективности защиты информации от утечки по техническим каналам;
- изучение методов и средств оценки защищенности выделенных (защищаемых) помещений и соответствия их нормативным документам;
- обучение основам построения системы технической защиты информации на критически важных объектах.

2. Место дисциплины в структуре образовательной программы

Дисциплина «Инженерно-техническая защита информации и технические средства на критически важных объектах» относится к базовой части. Требования к предшествующим знаниям представлены в таблице 2.1. Перечень дисциплин, для которых дисциплина «Инженерно-техническая защита информации и технические средства на критически важных объектах» является основополагающей, представлен в табл. 2.2.

Таблица 2.1 – Требования к пререквизитам дисциплины

Компетенция	Дисциплина
ОК-8	Курс полного школьного среднего образования.
ПСК – 3.2	Физика, информатика, Курс полного школьного среднего образования.

Таблица 2.2 – Требования к постреквизитам дисциплины

Компетенция	Дисциплина
ОК-8	Основы управленческой деятельности Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты (работа специалиста)
ПСК – 3.2	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
ОК-8 - способностью к самоорганизации и самообразованию	Этап 1: базовые понятия самоорганизации	Этап 1: использовать методы и средства самоорганизации	Этап 1: практические навыки использования методов самоорганизации
ОК-8 - способностью к самоорганизации и самообразованию	Этап 2: базовые понятия самообразования	Этап 2: использовать методы и средства самообразования	Этап 2: практические навыки использования методов самообразования
ПСК – 3.2 способностью участвовать в разработке, осуществлять внедрение и эксплуатацию средств защиты информации, используемых на критически важных объектах и в автоматизированных системах критически важных объектов	Этап 1: основные операционные системы, системы управления базами данных	Этап 1: выполнять комплекс задач администрирования подсистемы безопасности	Этап 1: выполнения комплекса задач администрирования подсистем безопасности
ПСК – 3.2 способностью участвовать в разработке, осуществлять внедрение и эксплуатацию средств защиты информации, используемых на критически важных объектах и в автоматизированных системах критически важных объектов	Этап 2: комплекс задач при администрировании подсистем информационной безопасности	Этап 2: выполнять комплекс задач по безопасности операционных систем и баз данных	Этап 2: выполнения администрирования компьютерных сетей по безопасности

4. Объем дисциплины

Объем дисциплины «Инженерно-техническая защита информации и технические средства на критически важных объектах» составляет 3 зачетные единицы (108 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 № 8	
				КР	СР
1	2	3	4	5	6
1	Лекции (Л)	18		18	
2	Лабораторные работы (ЛР)	18		18	
3	Практические занятия (ПЗ)	16		16	
4	Семинары(С)				
5	Курсовое проектирование (КП)				
6	Рефераты (Р)				
7	Эссе (Э)				
8	Индивидуальные домашние задания (ИДЗ)				
9	Самостоятельное изучение вопросов (СИВ)		26		26
10	Подготовка к занятиям (ПкЗ)		28		28
11	Промежуточная аттестация	2		2	
12	Наименование вида промежуточной аттестации	х	х	зачет	
13	Всего	54	54	54	54

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 Способы и средства добывания информации с помощью технических средств. Технические каналы утечки информации	8	10	10	8			х		12	14	х	ПСК – 3.2 ОК-8
1.1.	Тема 1 Сущность и задачи инженерно-технической защиты информации. Классификация, структура и характеристики технических каналов утечки информации.	8	2					х			2	х	ПСК – 3.2 ОК-8
1.2.	Тема 2 Оптические каналы утечки информации	8	2	2	2			х		2	2	х	ПСК – 3.2
1.3.	Тема 3 Акустические каналы утечки информации	8	2	2	2			х		2	4	х	ПСК – 3.2
1.4.	Тема 4 Радиоэлектронные каналы утечки информации. Каналы утечки информации, обрабатываемой средствами вычислительной техники.	8	2	4	2			х		4	4	х	ПСК – 3.2

№ 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
1.5.	Тема 5 Материально-вещественные каналы утечки информации	8	2	2	2			x		4	2	x	ПСК – 3.2 ОК-8
2	Раздел 2 Способы и средства защиты информации от утечки по техническим каналам. Разработка системы инженерно-технической защиты информации.	8	8	8	8			x		14	14	x	ПСК – 3.2 ОК-8
2.1.	Тема 6 Способы и средства защиты информации от наблюдения и подслушивания.	8	2	4	2			x		6	4	x	ПСК – 3.2 ОК-8
2.2.	Тема 7 Способы и средства защиты информации, обрабатываемой средствами вычислительной техники	8	2	4	2			x		4	4	x	ПСК – 3.2
2.3.	Тема 8 Системный подход к инженерно-технической защите информации	8	2		2			x			2	x	ПСК – 3.2 ОК-8
2.4.	Тема 9 Разработка системы инженерно-технической защиты информации на критически важных объектах	8	2		2			x		4	4	x	ПСК – 3.2 ОК-8
3	Контактная работа		18	18	16			x				2	x
4.	Самостоятельная работа									26	28		x
5.	Объем дисциплины в семестре		18	18	16					26	28	2	x
6.	Всего по дисциплине	x	18	18	16					26	28	2	x

5.2. Содержание дисциплины

5.2.1 – Темы лекций

№ п.п.	Наименование темы лекции	Объем, академические часы
Л-1	Сущность и задачи инженерно-технической защиты информации. Классификация, структура и характеристики технических каналов утечки информации.	2
Л-2	Оптические каналы утечки информации	2
Л-3	Акустические каналы утечки информации	2
Л-4	Радиоэлектронные каналы утечки информации. Каналы утечки информации, обрабатываемой средствами вычислительной техники.	2
Л-5	Материально-вещественные каналы утечки информации	2
Л-6	Способы и средства защиты информации от наблюдения и подслушивания.	2
Л-7	Способы и средства защиты информации, обрабатываемой средствами вычислительной техники	2
Л-8	Системный подход к инженерно-технической защите информации	2
Л-9	Разработка системы инженерно-технической защиты информации на критически важных объектах	2
Итого по дисциплине		18

5.2.2 – Темы лабораторных работ

№ п.п.	Наименование темы лабораторной работы	Объем, академические часы
ЛР-1	Ознакомление со средствами добывания информации в оптическом диапазоне волн	2
ЛР-2	Ознакомление со средствами добывания информации в акустическом диапазоне волн	2
ЛР-3	Ознакомление со средствами добывания информации в радиоэлектронном канале утечки	2
ЛР-4	Ознакомление со средствами добывания информации в электромагнитном канале утечки	2
ЛР-5	Изучение способов утечки информации по материально-вещественному каналу.	2
ЛР-6	Способы и средства защиты информации от наблюдения	2
ЛР-7	Способы и средства защиты информации, обрабатываемой средствами вычислительной техники и автоматизированными системами	2
ЛР-8	Методы и средства выявления электронных устройств негласного получения информации	2

ЛР-9	Методы и средства контроля эффективности защиты выделенных помещений от утечки речевой информации по техническим каналам	2
Итого по дисциплине		18

5.2.3 – Темы практических занятий

№ п.п.	Наименование темы занятия	Объем, академические часы
ПЗ-1	Выбор объекта и определение информационных ресурсов.	2
ПЗ-2-3	Разработка технического паспорта объекта	4
ПЗ-4	Моделирование каналов утечки информации	2
ПЗ-5	Разработка модели нарушителя технических каналов утечки информации для объекта защиты.	2
ПЗ-6	Разработка модели угроз технических каналов утечки информации для объекта защиты.	2
ПЗ-7-8	Разработка рекомендаций по выбору и установке технических средств защиты информации на критически важном объекте.	4
Итого по дисциплине		16

5.2.4 – Вопросы для самостоятельного изучения

№ п.п.	Наименования темы	Наименование вопроса	Объем, академические часы
1.	Оптические каналы утечки информации	Способы перехвата информации в волоконно-оптических линиях связи	2
2.	Акустические каналы утечки информации	Особенности перехвата информации в телефонных линиях сотовой связи	2
3.	Радиоэлектронные каналы утечки информации. Каналы утечки информации, обрабатываемой средствами вычислительной техники.	Специально создаваемые технические каналы утечки информации	4
4.	Материально-вещественные каналы утечки информации	Особенности утечки информации о радиоактивных веществах.	4
5.	Способы и средства защиты информации от наблюдения и подслушивания.	Методика расчета словесной разборчивости речи.	4
6.	Способы и средства защиты информации от наблюдения и подслушивания.	Системы пространственного и линейного электромагнитного зашумления	2
7.	Способы и средства защиты информации, обрабатываемой средствами вычислительной	Методы и средства пассивного подавления опасных сигналов	4

	техники	акустоэлектрических преобразователей.	
8.	Разработка системы инженерно-технической защиты информации на критически важных объектах	САПР систем технической защиты информации.	4
Итого по дисциплине			26

6. Учебно-методическое и информационное обеспечение дисциплины

6.1 Основная учебная литература, необходимая для освоения дисциплины

1. Методы и средства инженерно-технической защиты информации [Электронный ресурс]: учебное пособие/ В.И. Аверченков [и др.].— Электрон. текстовые данные.— Брянск: Брянский государственный технический университет, 2012.— 187 с.

2. 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.

6.2 Дополнительная учебная литература, необходимая для освоения дисциплины

1. Титов А. А. Инженерно-техническая защита информации. Учебное пособие [Электронный ресурс] / Титов А. А. - Томский государственный университет систем управления и радиоэлектроники, 2010.

2. Креопалов В. В. Технические средства и методы защиты информации. Учебно-практическое пособие [Электронный ресурс] / Креопалов В. В. - Евразийский открытый институт, 2011.

6.3 Методические материалы для обучающихся по освоению дисциплины

Электронное учебное пособие, включающее:

- конспект лекций;
- методические материалы по выполнению лабораторных работ;
- 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 для студентов 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. Open Office
2. JoliTest (JTRun, JTEditor, TestRun)
3. ПО, поставляемое совместно с техническими средствами защиты информации.

6.6 Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

1. <http://www.analitika.info> Средства защиты информации. Каталог техники выявления и противодействия средствам разведки, антитеррора. Форум по вопросам защиты информации.
2. <http://www.fstec.ru> Официальный сайт Федеральной службы по техническому и экспортному контролю (ФСТЭК России).
3. <http://www.fsb.ru> Федеральная Служба безопасности Российской Федерации.
4. <http://clsz.fsb.ru> Центр по лицензированию, сертификации и защите государственной тайны ФСБ России.
5. <http://www.consultant.ru> Общероссийская Сеть распространения правовой информации КонсультантПлюс
6. <http://www.bnti.ru/about.asp> Бюро научно-технической информации. Техника для спецслужб.

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

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

Таблица 7.1 – Материально-техническое обеспечение лабораторных работ

Номер ЛР	Тема лабораторной работы	Название специализированной лаборатории	Название спецоборудования	Название технических и электронных средств обучения и контроля знаний
1	2	3	4	5
ЛР-1	Ознакомление со средствами добывания информации в оптическом диапазоне волн	948 аудитория ИУР и КБ	персональный компьютер	Специализированные программные средства
ЛР-2	Ознакомление со средствами добывания информации в акустическом диапазоне волн	948 аудитория ИУР и КБ	персональный компьютер	Специализированные программные средства
ЛР-3	Ознакомление со средствами добывания информации в радиоэлектронном канале утечки	948 аудитория ИУР и КБ	персональный компьютер	Специализированные программные средства
ЛР-4	Ознакомление со средствами добывания информации в	948 аудитория ИУР и КБ	персональный компьютер	Специализированные программные средства

	электромагнитном канале утечки			
ЛР-5	Изучение способов утечки информации по материально-вещественному каналу.	948 аудитория ИУР и КБ	персональный компьютер	Специализированные программные средства
ЛР-6	Способы и средства защиты информации от наблюдения	948 аудитория ИУР и КБ	оптический обнаружитель скрытых видеокамер «Оптик» автоматический обнаружитель видеокамер «Айрис IQ-2V» персональный компьютер	Специализированные программные средства
ЛР-7	Способы и средства защиты информации, обрабатываемой средствами вычислительной техники и автоматизированными системами	948 аудитория ИУР и КБ	детектор электромагнитного поля ST 110, персональный компьютер	Специализированные программные средства
ЛР-8	Методы и средства выявления электронных устройств негласного получения информации	948 аудитория ИУР и КБ	многофункциональный поисковый прибор ST 031P «Пиранья», персональный компьютер	Специализированные программные средства
ЛР-9	Методы и средства контроля эффективности защиты выделенных помещений от утечки речевой информации по техническим каналам	948 аудитория ИУР и КБ	многофункциональный поисковый прибор ST 031P «Пиранья», персональный компьютер	Специализированные программные средства

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.

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.

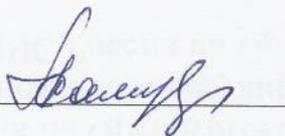
Самостоятельная работа студентов проводится в помещениях для самостоятельной работы, укомплектованном специализированной мебелью и техническими средствами

обучения. Учебное оборудование хранится и обслуживается в помещениях для хранения и профилактического обслуживания учебного оборудования.

Оценочные материалы для проведения промежуточной аттестации обучающихся по дисциплине представлен 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 от 1 декабря 2016 г. №1509.

Разработал(и): _____



Е. В. Каменева