Министерство образования и науки Российской Федерации

Федеральное государственное бюджетное образовательное учреждение высшего образования

Пермский национальный исследовательский политехнический университет

Электротехнический факультет
Кафедра автоматики и телемеханики

УТВЕРЖДАЮ
Проректор по учебной работе
д-р техн. наук, проф.
_____ Н. В. Лобов
«14» 04 201_ г.

УЧЕБНО-МЕТОДИЧЕСКИЙ КОМПЛЕКС ДИСЦИПЛИНЫ
«Техническая защита информации»

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Программа специалитета

Специальность 10.05.03 Информационная безопасность автоматизированных систем

Специализация Обеспечение информационной безопасности распределенных информационных систем

Квалификация выпускника: Специалист по защите информации

Выпускающая кафедра: Автоматика и телемеханика

Форма обучения: очная

Курс: 4 **Семестр:** 7

Трудоёмкость:
Кредитов по рабочему учебному плану: 4 ЗЕ
Часов по рабочему учебному плану: 144 ч

Виды контроля: Экзамен - 7 семестр

Пермь 2017

Рабочая программа дисциплины «Техническая защита информации» разработана на основании:

- Федерального государственного образовательного стандарта высшего образования по специальности 10.05.03 Информационная безопасность автоматизированных систем (уровень специалитета), утвержденного приказом Министерства образования и науки Российской Федерации от «01» декабря 2016 г. № 1509;
- Компетентностной модели выпускника образовательной программы высшего образования – программы по специальности 10.05.03 Информационная безопасность автоматизированных систем, специализации «Обеспечение информационной безопасности распределенных информационных систем», утвержденной «24» июня 2013 г. (с изменениями, в связи с переходом на ФГОС ВО);
- Базового учебного плана очной формы обучения образовательной программы высшего образования – программы по специальности 10.05.03 Информационная безопасность автоматизированных систем, специализации «Обеспечение информационной безопасности распределенных информационных систем», утвержденного «22» декабря 2016 г.

Рабочая программа согласована с рабочими программами дисциплин, участвующих в формировании компетенций и их составляющих, приобретение которых является целью данной дисциплины:

Комплексная защита информации на предприятии, Криптографические методы защиты информации, Разработка и эксплуатация защищенных автоматизированных систем, Технические средства охраны, Программно-аппаратные средства защиты информации.

Разработчик: доц. _____ В.П. Костецкий

Рецензент: канд. техн. наук, доц. _____ А.С. Шабуров

Рабочая программа рассмотрена и одобрена на заседании кафедры «Автоматика и телемеханика» «16» 01 2017 г., протокол № 18

Заведующий выпускающей
кафедрой «Автоматика и телемеханика»,
доктор техн. наук., проф. _____ А.А.Южаков

Рабочая программа рассмотрена и одобрена учебно-методической комиссией электротехнического факультета «6» 02 2017 г.,
протокол № 1.

Председатель учебно-методической комиссии
электротехнического факультета,
канд. техн. наук, проф. _____ А. Л. Гольдштейн

СОГЛАСОВАНО
Начальник управления образовательных
программ, канд. техн. наук, доц. _____ Д. С. Репецкий

1 Общие положения

1.1 Цель дисциплины - формирование знаний в области принципов добывания (разведки) информации, способов организационно-технической и технической защиты информации, активных и пассивных способов и средств скрытия и защиты, способов и средств технической дезинформации, принципов технического контроля защищенности объектов.

В процессе изучения дисциплины студент осваивает следующие дисциплинарные компетенции:

способность разрабатывать и анализировать проектные решения по обеспечению безопасности автоматизированных систем (ПК-8);

способность участвовать в разработке защищенных автоматизированных систем в сфере профессиональной деятельности (ПК-9);

способность участвовать в проектировании средств защиты информации автоматизированной системы (ПК-13).

1.2 Задачи дисциплины:

• изучение систем и средств инженерно-технической разведки, методов и способов организации защиты объектов активными и пассивными способами и техническими средствами, выбора оптимальных (по условиям эксплуатации и экономичности) технических средств защиты информации, нормативно-методических и правовых документов, регламентирующих вопросы технической защиты информации;

• формирование умения выявлять каналы утечки на конкретных объектах и оценивать их возможности;

• формирование умения определять рациональные меры защиты на объектах и оценивать уровень эффективности их защиты;

• формирование владения:

- методами организации защиты объектов активными и пассивными способами и техническими средствами;

- методами выбора оптимальных (по условиям эксплуатации и экономичности) технических средств защиты информации;

- методами работы с техническими средствами контроля безопасности информации;

- методами выбора и поиска технических решений защиты объектов информации.

1.3 Предметом освоения дисциплины являются следующие объекты:

Объекты информатизации, включая компьютерные, автоматизированные, телекоммуникационные, информационные ресурсы и информационные технологии, в условиях существования угроз в информационной сфере;

технологии обеспечения информационной безопасности объектов различного уровня (система, объект системы, компонент объекта), которые связаны с информационными технологиями, используемыми на этих объектах;

процессы управления информационной безопасностью защищаемых объектов.

1.4 Место учебной дисциплины в структуре образовательной программы

Дисциплина «**Техническая защита информации**» относится к базовой части Блок 1 и является обязательной дисциплиной при освоении ООП по профилю «Комплексная защита объектов информатизации».

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

- Знать:
  - принципы и методы организационной защиты информации;
  - технические каналы утечки информации;
  - возможности технических разведок;
  - способы и средства защиты информации от утечек по техническим каналам;
  - физические явления и эффекты, используемые при обеспечении информационной безопасности автоматизированных систем;
  - формы и способы представления данных в персональном компьютере;
  - универсальные приемы исследования оптимизационных проблем при различной степени неопределенности условий.
- Уметь:
  - анализировать и оценивать угрозы информационной безопасности объекта;
  - пользоваться нормативными документами по защите информации;
  - анализировать и применять физические явления и эффекты для решения практических задач обеспечения информационной безопасности;
  - решать типовые прикладные физические задачи;

– применять нормативные документы по метрологии, стандартизации и сертификации на практике.

- Владеть:

- методами и средствами выявления угроз безопасности автоматизированным системам;

- методами технической защиты информации;

- методами формирования требований по защите информации;

- методами расчета и инструментального контроля показателей технической защиты информации;

- навыками обеспечения безопасности информации с помощью типовых программных и технических средств;

- навыками разработки документации по метрологии, стандартизации и сертификации программных и аппаратных средств защиты.

В таблице 1 приведены предшествующие и последующие дисциплины, направленные на формирование компетенций, заявленных в пункте 1.1.

Таблица 1 – Дисциплины, направленные на формирование компетенций

Код	Наименование компетенции	Предшествующие дисциплины	Последующие дисциплины (группы дисциплин)
Профессиональные компетенции			
ПК-8	Способность разрабатывать и анализировать проектные решения по обеспечению безопасности автоматизированных систем	Математика (Математический анализ). Математика (Алгебра и геометрия). Теория вероятностей, математическая статистика и случайные процессы. Физика. Информатика. Теория информации. Физические основы микроэлектроники. Теория систем массового обслуживания. Прикладные задачи в области инфокоммуникационных и информационно-управляющих систем. Физико-технические эффекты Физика колебаний и волн Основы информационной безопасности История защиты информации Криптографические методы защиты информации Организационное и правовое обеспечение информационной безопасности Вычислительная техника и информационные технологии Основы построения инфокоммуникацион-	Комплексная защита информации на предприятии. Информационная безопасность в банковской системе. Внутренний аудит систем защиты информации на соответствие стандартам. Разработка и эксплуатация защищенных автоматизированных систем. Управление информационной безопасностью Разработка и эксплуатация защищенных автоматизированных систем

		ных систем и сетей Электроника и схемотехника (Электроника) Электротехника (Электропитание устройств и систем) Программно-аппаратные средства защиты информации Комплексная защита информации на предприятии Защита и обработка конфиденциальных документов Технические средства охраны Теория электрических цепей Электромагнитные поля и волны Метрология, стандартизация и сертификация	
ПК-9	Способность участвовать в разработке защищенных автоматизированных систем в сфере профессиональной деятельности	Физика. Информатика. Теория информации. Физико-технические эффекты Физика колебаний и волн Основы информационной безопасности Криптографические методы защиты информации Организационное и правовое обеспечение информационной безопасности Вычислительная техника и информационные технологии Основы построения инфокоммуникационных систем и сетей Электроника и схемотехника (Электроника) Электротехника (Электропитание устройств и систем) Программно-аппаратные средства защиты информации Комплексная защита информации на предприятии Защита и обработка конфиденциальных документов Технические средства охраны Теория электрических цепей Электромагнитные поля и волны Метрология, стандартизация и сертификация	Комплексная защита информации на предприятии Внутренний аудит систем защиты информации на соответствие стандартам. Программно-аппаратные средства защиты информации. Разработка и эксплуатация защищенных автоматизированных систем. Информационно-аналитическое обеспечение безопасности предприятия. Теория информационной безопасности и методология защиты информации. Управление информационной безопасностью Разработка и эксплуатация защищенных автоматизированных систем

ПК-13	Способность участвовать в проектировании средств защиты информации автоматизированной системы	Физика. Информатика. Теория информации. Физические основы микроэлектроники. Физико-технические эффекты Физика колебаний и волн Основы информационной безопасности Криптографические методы защиты информации Организационное и правовое обеспечение информационной безопасности Вычислительная техника и информационные технологии Основы построения инфокоммуникационных систем и сетей Электроника и схемотехника (Электроника) Электротехника (Электропитание устройств и систем) Программно-аппаратные средства защиты информации Комплексная защита информации на предприятии Метрология, стандартизация и сертификация	Программно-аппаратные средства защиты информации. Разработка и эксплуатация защищенных автоматизированных систем. Теория информационной безопасности и методология защиты информации. Управление информационной безопасностью Разработка и эксплуатация защищенных автоматизированных систем

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

Учебная дисциплина обеспечивает формирование части компетенций ПК-8 - ПК-8- Б1.Б.24, ПК-9- ПК-9- Б1.Б.24, ПК-13- ПК-13- Б1.Б.24.

2.1 Дисциплинарная карта компетенции ПК-1- Б1.Б.24

Код	Формулировка компетенции:
ПК-8	Способность разрабатывать и анализировать проектные решения по обеспечению безопасности автоматизированных систем

Код	Формулировка дисциплинарной части компетенции:
ПК-8. Б1.Б.24	Способность организовать и поддерживать выполнение комплекса мер по информационной безопасности, выявлять угрозы безопасности автоматизированных систем, владеть методами технической защиты информации, методами расчета и инструментального контроля показателей технической защиты информации.

Требования к компонентному составу части компетенции

Перечень компонентов	Виды учебной работы	Средства оценки
В результате освоения части компетенции студент **Знает:** Принципы и методы организационной защиты информации. Технические каналы утечки информации. Возможности технических разведок. Способы и средства защиты информации от утечек по техническим каналам.	Лекции. Самостоятельная работа студентов по изучению теоретического материала.	Тестовые вопросы для текущего и рубежного контроля.
Умеет: Анализировать и оценивать угрозы информационной безопасности объекта. Пользоваться нормативными документами по защите информации.	Практические занятия. Лабораторные работы. Самостоятельная работа студентов по решению практических задач.	Практические задания к контрольным работам. Отчёт по ЛР.
Владеет: Методами и средствами выявления угроз безопасности автоматизированным системам. Методами технической защиты информации. Методами формирования требований по защите информации. Методами расчета и инструментального контроля показателей технической защиты информации.	Самостоятельная работа по подготовке к зачёту / экзамену.	Отчёт. Вопросы к зачёту / экзамену.

2.2 Дисциплинарная карта компетенции ПК-5. Б1.Б.24

Код	Формулировка компетенции:
ПК-9	Способность участвовать в разработке защищенных автоматизированных систем в сфере профессиональной деятельности

Код	Формулировка дисциплинарной части компетенции:
ПК-9. Б1.Б.24	Способность владеть методиками проверки защищенности объектов информатизации на соответствие требованиям нормативных документов.

Требования к компонентному составу части компетенции

Перечень компонентов	Виды учебной работы	Средства оценки
В результате освоения части компетенции студент **Знает:** Принципы организации информационных систем в соответствии с требованиями по защите информации. Принципы и методы организационной защиты информации. Технические каналы утечки информации, возможности технических разведок, способы и средства защиты информации от утечки по техническим каналам, методы и средства контроля эффективности технической защиты информации.	Лекции. Самостоятельная работа студентов по изучению теоретического материала.	Тестовые вопросы для текущего и рубежного контроля.
Умеет: Анализировать и оценивать угрозы информационной безопасности объекта. Пользоваться нормативными документами по защите информации.	Практические занятия. Лабораторные работы. Самостоятельная работа студентов по решению практических задач.	Практические задания к контрольным работам. Отчёт по ЛР.
Владеет: Методами и средствами выявления угроз безопасности автоматизированных систем. Методами технической защиты информации. Методами расчета и инструментального контроля показателей технической защиты информации. Методиками проверки защищенности объектов информатизации на соответствие требованиям нормативных документов.	Самостоятельная работа по подготовке к зачёту / экзамену.	Отчёт. Вопросы к зачёту / экзамену.

2.3 Дисциплинарная карта компетенции ПК-6. Б1.Б.24

Код	Формулировка компетенции:
ПК-13	Способность участвовать в проектировании средств защиты информации автоматизированной системы

Код	Формулировка дисциплинарной части компетенции:
ПК-13. Б1.Б.24	Способность осуществлять меры противодействия нарушителям информационной безопасности с использованием различных программных и аппаратных средств защиты.

Требования к компонентному составу части компетенции

Перечень компонентов	Виды учебной работы	Средства оценки
В результате освоения части компетенции студент **Знает:** Принципы организации информационных систем в соответствии с требованиями по защите информации. Технические каналы утечки информации, возможности технических разведок, способы и средства защиты информации от утечки по техническим каналам, методы и средства контроля эффективности технической защиты информации.	Лекции. Самостоятельная работа студентов по изучению теоретического материала.	Тестовые вопросы для текущего и рубежного контроля.
Умеет: Анализировать и оценивать угрозы информационной безопасности объекта. Формулировать и настраивать политику безопасности распространенных операционных систем, а также локальных вычислительных сетей, построенных на их основе. Осуществлять меры противодействия нарушителям сетевой безопасности с использованием различных программных и аппаратных средств защиты.	Практические занятия. Лабораторные работы. Самостоятельная работа студентов по решению практических задач.	Практические задания к контрольным работам. Отчёт по ЛР.
Владеет: Методами и средствами выявления угроз безопасности автоматизированных систем. Методами технической защиты информации. Методами расчета и инструментального контроля показателей технической защиты информации. Методиками проверки защищенности объектов информатизации на соответствие требованиям нормативных документов.	Самостоятельная работа по подготовке к зачёту / экзамену.	Отчёт. Вопросы к зачёту / экзамену.

3 Структура учебной дисциплины по видам и формам учебной работы

Таблица 2 – Объём и виды учебной работы

№ п.п.	Виды учебной работы	Трудоёмкость		
		по семестрам		всего
1	2	3	4	5
1	**Аудиторная (контактная) работа** - в том числе в интерактивной форме	54 -		54 -
	Лекции (Л) - в том числе в интерактивной форме	24 -		24 -
	Практические занятия (ПЗ) - в том числе в интерактивной форме	8 -		8 -
	Лабораторные работы (ЛР) - в том числе в интерактивной форме	20 -		20 -
2	Контроль самостоятельной работы (КСР)	2		2
3	**Самостоятельная работа студентов** (СРС)	54		54
	Изучение теоретического материала	26		26
	Расчётно-графические работы			

	Индивидуальные задания *(курсовой проект (работа) / реферат / .....)*			
	Другие виды самостоятельной работы: - подготовка к практическим занятиям - подготовка к лабораторным работам	 8 20		 8 20
4	Итоговый контроль (промежуточная аттестация обучающихся) по дисциплине: *зачёт /экзамен*	36		0 / 36
5	**Трудоёмкость дисциплины** **Всего:** **в часах (ч)** **в зачётных единицах (ЗЕ)**	 144 4		 144 4

4 Содержание учебной дисциплины

4.1 Модульный тематический план

Таблица 3 – Тематический план по модулям учебной дисциплины

Номер учебного модуля	**Номер раздела дисциплины**	**Номер темы дисциплины**	**Количество часов и виды занятий (очная форма обучения)**							**Трудоёмкость, ч / ЗЕ**
			аудиторная работа					**Итоговый контроль**	**самостоятельная работа**	
			всего	**Л**	**ПЗ**	**ЛР**	**КСР**			
1	2	3	4	5	6	7	8	9	10	11
1	1	Введение	1	1						
		1	2	2					ИТМ- 4	
		2	4	2		2			ППЗ -2	
	2	3	4	2		2			ППЗ -4	
		4	8	2	2	4			ППЗ -2 ПЛР-4	
	3	5	2	2					ИТМ-2	
		6	2	2					ИТМ- 2	
	Всего по модулю:			**13**	**2**	**8**		**12**	**20**	
2	4	7	6	2		4			ИТМ-4 ПЛР -4	
		8	8	2	2	4			ИТМ -2 ППЗ -4 ПЛР -4	
	Всего по модулю:			**4**	**2**	**8**	**1**	**12**	**18**	
3	5	9	4	2		2			ИТМ-2 ПЛР -2	
		10	4	2		2			РТМ -4 ППЗ -2	
		11	6	2	4				ИТМ -2 ППЗ -2 ПЛР -2	
		Заключение	1	1				2		**1**

Всего по модулю:		**7**	**4**	**4**	**1**	**12**	**16**	
Итоговая аттестация						**36**		**36**
Итого:	**54**	**24**	**8**	**20**	**2**	**36**	**54**	

** ИТМ - изучение теоретического материала;*
ППЗ - подготовка к практическим занятиям;
ПЛР – подготовка к лабораторной работе.

4.2 Содержание разделов и тем учебной дисциплины

Введение.

Л – 1 ч.

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

Связь курса с другими дисциплинами специальности. Структура курса, его роль и место в подготовке специалистов по защите информации. Рекомендуемые учебные пособия.

Виды, источники и носители защищаемой информации. Классификация иностранной технической разведки.

Возможности видов технической разведки.

Основные этапы и процедуры добывания информации технической разведкой. Задачи систем защиты информации.

Модуль 1. Виды, методы и средства технической разведки.

Раздел 1. Цели, задачи и организация технической разведки. Радиоэлектронная и оптическая разведки.

Л – 4 ч, ЛР – 2 ч, СРС – 6 ч.

Тема 1. **Цели, задачи и организация технической разведки. Радиоэлектронная разведка.**

Понятие технической разведки. Цели, задачи, принципы организации технической разведки. Каналы утечки информации.

Классификация технических разведок по видам носителей аппаратуры разведки.

Классификация технических разведок по способу добывания информации и типу аппаратуры разведки.

Общая характеристика радиоэлектронной разведки, ее особенности, основные показатели технических средств радио-радиотехнической, радиолокационной и радиотепловой разведки и разведки побочных электромагнитных излучений и наводок. Выбор стратегий разведки и маскировки. Заметность радиоизлучения и эффективность разведки. Структурная схема станции

радиотехнической разведки. Способы определения частоты сигналов РЭС. Пеленгация радиоэлектронных средств.

Порядок ведения радиолокационной разведки. Структурная схема и основные показатели станции радиолокационной разведки. Фоновая радиолокация.

Метод когерентной оптической обработки сигналов радиолокационных станций с синтезированной апертурой.

Порядок ведения радиотепловой разведки. Структурная схема и основные показатели станции радиотепловой разведки.

Разведка побочных электромагнитных излучений и наводок. Перехват информации с кабельных линий связи. Перехват информации по побочным излучениям со средств ЭВТ. Перехват информации за счет наводок. Перехват информации методом высокочастотного навязывания. Перехват информации за счет микрофонного эффекта. Перехват информации за счет паразитных излучений устройств, не имеющих электроакустических систем. Перехват информации с волоконно-оптических линий связи.

Тема 2. **Оптическая разведка.**

Общие сведения об оптических линзовых системах. Сущность излучения объектов в инфракрасном диапазоне. Электронноптические преобразователи.

Порядок ведения и основные показатели визуально-оптической разведки.

Порядок ведения и основные показатели фотографической и фототелевизионной разведки.

Порядок ведения и основные показатели телевизионной разведки.

Тепловидение. Теплопеленгация.

Оптическая (лазерная) локация. Структурная схема дальномерного канала.

Раздел 2. Технические средства негласного получения информации.

Л – 4 ч, ПЗ – 2 ч, ЛР – 6 ч, СРС – 10 ч.

Тема 3. Технические средства негласного получения акустической (речевой) информации.

Технические средства акустической разведки, их функции.

Направленные микрофоны. Назначение и основные характеристики. Параболический микрофон. Плоские фазированные решетки. Микрофон – труба. Трубчатые микрофоны «бегущей волны».

Проводные микрофонные системы.

Игольчатые микрофоны и электронные стетоскопы.5

Лазерные акустические системы разведки.

Микрофонный эффект в основных и вспомогательных технических средствах.

Обработка перехваченных речевых сигналов.

Акустические закладные устройства. Радиозакладки. Диктофоны. Акустические закладки, использующие телефонные линии.

Тема 4. Технические средства для негласного перехвата и регистрации информации с технических каналов связи. Специальные технические средства для негласного получения (изменения, уничтожения) информации с технических средств ее хранения, обработки и передачи.

Электромагнитные, электрические и параметрические каналы перехвата информации. Параметры линий связи. Расчет помех (наводок) в каналах связи.

Способы и средства перехвата сигналов связи. Структура типового комплекса средств перехвата. Возможности по перехвату радиосигналов в диапазонах частот. Средства измерения признаков сигнала.

Средства перехвата факсимильных сообщений. Системы контроля сотовой связи, пейджинговой связи, телексной связи.

Системы перехвата сигналов с компьютерных сетей и контроля телекоммуникаций:

- аппаратные закладки для перехвата видеоизображений;
- аппаратные закладки для перехвата информации, вводимой с клавиатуры ПЭВМ.

Раздел 3. Технические средства негласного слежения и проникновения на объект.

Л – 4 ч, СРС – 4 ч.

Тема 5. Специальные технические средства для негласного исследования предметов и документов. Специальные технические средства для негласного проникновения на объект.

. Средства преодоления конвертовой защиты.

Специальные эндоскопы.

Средства выявления маркерной защиты.

Средства выявления естественных следов:

Специальные технические средства для негласного проникновения на объект.

Средства диагностики запирающих устройств:

- специальные эндоскопы для визуального осмотра механических замков через замочные скважины;
- средства акустической и виброакустической диагностики механических, и в частности, кодовых сейфовых замков;
- специальные средства электромагнитной диагностики электромеханических кодовых запирающих устройств.

Специальный слесарный инструмент.

Тема 6. Системы слежения за транспортными средствами

Системы определения местоположения, использующие методы спутниковой радионавигации.

Системы слежения за транспортными средствами.

Компании, предоставляющие услуги в сфере спутниковых навигационных технологий.

Модуль 2. Технические каналы утечки информации.

Раздел 4. Технические каналы утечки речевой, обрабатываемой ТСПИ, передаваемой по каналам связи и видовой информации.

Л – 4 ч, ПЗ – 2 ч, ЛР – 8 ч, СРС – 18 ч, КСР – 1 ч.

Тема 7. Технические каналы утечки речевой информации.

Краткие сведения по акустике. Звуковое поле. Линейные характеристики звукового поля. Энергетические характеристики звукового поля. Плоская волна. Сферическая волна. Акустические и электрические уровни.

Звуковые сигналы. Маскировка звуковых сигналов.

Понятность и разборчивость речи.

Частотный диапазон и спектры.

Звуковое поле в помещении. Звуковой фон в помещении.

Характеристики помещения

Звукопоглощающие материалы и конструкции.

Звукоизоляция помещений.

Акустические каналы утечки речевой информации.

Микрофоны. Направленные микрофоны. Проводные системы.

Портативные диктофоны и электронные стетоскопы.

Радиомикрофоны. Гидроакустические датчики.

СВЧ и ИК передатчики.

Виброакустические технические каналы утечки речевой информации.

Акустоэлектрические каналы утечки речевой информации.

Оптико-электронный технический канал утечки речевой информации.

Параметрические технические каналы утечки речевой информации

Тема 8. Технические каналы утечки информации, обрабатываемой ТСПИ и передаваемой по каналам связи. Технические каналы утечки видовой информации

Физическая природа побочных электромагнитных излучений.

Элементарный электрический излучатель.

Элементарный магнитный излучатель.

Электромагнитные каналы утечки информации ТСПИ.

Электрические каналы утечки информации.
Наводки электромагнитных излучений ТСПИ.
Параметрический канал утечки информации.
Технические каналы утечки информации при передаче ее по каналам связи.

Электрические линии связи.

Средства передачи электрических сигналов.
Каналы утечки информации за счет паразитных связей.
Опасные сигналы и их источники.
Электрические каналы утечки информации.
Контроль и прослушивание телефонных каналов связи
Электромагнитные каналы утечки информации.
Индукционный канал утечки информации.
Демаскирующие признаки радиоэлектронных средств.
Демаскирующие признаки объектов в видимом диапазоне электромагнитного спектра.
Демаскирующие признаки объектов в инфракрасном диапазоне электромагнитного спектра. Способы скрытого видеонаблюдения и съемки.

Модуль 3. Средства защиты информации

Раздел 5. Пассивные и активные средства защиты информации. Принципы оценки эффективности систем инженерно-технической защиты информации.
Л – 6 ч, ПЗ – 4 ч, ЛР – 4 ч, СРС – 24 ч., КСР – 1 ч.

Тема 9. Пассивные средства защиты информации.
Методы и средства пассивной защиты.

Обеспечение безопасности мест хранения и обработки информации:
- автоматизированные контрольно-пропускные системы (в т.ч. с идентификацией личности) с использованием электромеханических запирающих и блокирующих устройств;
- системы защиты от НСД локальных и глобальных компьютерных сетей;
- автоматизированные системы контроля служебного документооборота (печати, архивации и пр.), электронной почты и т.п.

Защита линий связи и коммуникаций:
- криптографическая защита данных (по схеме шифрования с открытым ключом), передаваемых по линиям связи по стандартным протоколам (типа X-25 и др.);
- многоуровневое разграничение доступа к средствам и ресурсам;

- идентификация абонентов-пользователей (в частности, путем применения 8-32 значных паролей);

- функциональная замкнутость;
- возможность одновременной работы в реальном времени с большим числом абонентов (до нескольких сотен);
- антивирусная защита.

Нейтрализация каналов естественного (неумышленного) и искусственного (умышленного) хищения (разглашения) информации служащими.

Тема 10. Активные средства информационной защиты.

Методы и средства активной защиты:

- создание прицельных помех в канале утечки информации;
- снижение чувствительности (подавления или нейтрализация) датчиков каналов

утечки информации;
- кодирование сообщений;
- воздействия сильных электромагнитных, электрических, акустических, виброакустических и др. полей на каналы информационных хищений вне полосы частот информационных сигналов.

Тема 11. Принципы оценки эффективности систем инженерно-технической защиты информации.

Моделирование защиты информации. Модели системы защиты и показатели эффективности. Стоимость защиты. Рекомендации по выбору рациональных вариантов защиты информации и соответствующих технических средств.

Контроль эффективности мер по защите информации техническими средствами.

Технический контроль эффективности принимаемых мер защиты. Назначение, содержание, вид и методы технического контроля. Основные средства технического контроля.

Заключение.

Л – 1 ч.

Подведение итогов изучения дисциплины.

4.3 Перечень тем практических занятий

Таблица 4 – Темы практических занятий

№ п.п.	Номер темы дисциплины	Наименование темы практического занятия
1	2	3
1	4	Применение специальных технических средств перехвата сигналов связи и негласного получения (изменения, уничтожения) информации с технических средств ее хранения, обработки и передачи.
2	8	Оценка угроз перехвата информации, обрабатываемой ТСПИ по техническим каналам ПЭМИН.
3	11	Контроль эффективности мер по защите информации техническими средствами. Моделирование защиты информации.
4	11	Разработка рекомендаций по выбору рациональных вариантов защиты информации и соответствующих технических средств.

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	2	Радиомониторинг объекта информатизации (ПЭВМ), выявление информативных частот ПЭМИН с помощью комплекса «Навигатор П3».
2	3	Ведение акустической разведки с помощью акустического и виброакустического преобразователей многофункционального прибора «Пиранья» и комплекса «Аврора-2».
3	4	Радиомониторинг объекта информатизации (ПЭВМ), выявление информативных частот ПЭМИН с помощью комплекса «Навигатор П3».
4	7	Оценка эффективности постановки активных электромагнитных помех от генератора шума низкочастотного Г2-59 с помощью индикатора поля и комплекса «Крона».
5	8	Использование приборов физического поиска специальных технических средств разведки: -регистратора радиоволновых полей и оптических излучений (из комплекса «Пиранья»; - металло- и трассоискателей; - обнаружители импедансных изменений: телефонные проверочные устройства (Улан -2); - устройства поиска по функциональным признакам, акустозавязка (ST-006 и Пиранья); -устройство визуального контроля «Шмель».
6	9	Оценка эффективности защиты речевой информации в телефонных линиях связи за счет использования прибора комплексной защиты от прослушивания «Прокруст-2000».
7	10	Контроль эффективности активных и пассивных средств защиты ПЭВМ комплексом «Навигатор П3».

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.

Тематика для самостоятельного изучения дисциплины:

Введение. Основные понятия, термины и определения, предмет и задачи дисциплины. Структура изучения материала. Актуальность технической защиты информации.

Тема 1. **Цели, задачи и организация технической разведки. Радиоэлектронная разведка.**

Цели, задачи, принципы организации технической разведки. Каналы утечки информации.

Классификация технических разведок по видам носителей аппаратуры разведки.

Классификация технических разведок по способу добывания информации и типу аппаратуры разведки.

Общая характеристика радиоэлектронной разведки, ее особенности, основные показатели технических средств радио-радиотехнической, радиолокационной и радиотепловой разведки и разведки побочных электромагнитных излучений и наводок. Способы определения частоты сигналов РЭС. Пеленгация радиоэлектронных средств.

Тема 5. Специальные технические средства для негласного исследования предметов и документов. Специальные технические средства для негласного проникновения на объект.

. Средства преодоления конвертовой защиты.

Специальные эндоскопы.

Средства выявления маркерной защиты.

Средства выявления естественных следов:

Специальные технические средства для негласного проникновения на объект.

Средства диагностики запирающих устройств:

- специальные эндоскопы для визуального осмотра механических замков через замочные скважины;
- средства акустической и виброакустической диагностики механических, и в частности, кодовых сейфовых замков;
- специальные средства электромагнитной диагностики электромеханических кодовых запирающих устройств.

Специальный слесарный инструмент.

Тема 6. Системы слежения за транспортными средствами

Системы определения местоположения, использующие методы спутниковой радионавигации.

Системы слежения за транспортными средствами.

Компании, предоставляющие услуги в сфере спутниковых навигационных технологий.

Тема 7. Технические каналы утечки речевой информации.

Звуковое поле. Линейные характеристики звукового поля. Энергетические характеристики звукового поля. Плоская волна. Сферическая волна. Акустические и электрические уровни.

Звуковые сигналы. Маскировка звуковых сигналов.

Понятность и разборчивость речи.

Частотный диапазон и спектры.

Звуковое поле в помещении. Звуковой фон в помещении.

Звукопоглощающие материалы и конструкции.

Звукоизоляция помещений.

Акустические каналы утечки речевой информации.

Микрофоны. Направленные микрофоны. Проводные системы.

Портативные диктофоны и электронные стетоскопы.

Радиомикрофоны. Гидроакустические датчики.

СВЧ и ИК передатчики.

Виброакустические технические каналы утечки речевой информации.

Акустоэлектрические каналы утечки речевой информации.

Оптико-электронный технический канал утечки речевой информации.

Параметрические технические каналы утечки речевой информации

Тема 8. Технические каналы утечки информации, обрабатываемой ТСПИ и передаваемой по каналам связи. Технические каналы утечки видовой информации

Физическая природа побочных электромагнитных излучений.

Элементарный электрический излучатель.

Элементарный магнитный излучатель.

Электромагнитные каналы утечки информации ТСПИ.

Электрические каналы утечки информации.

Наводки электромагнитных излучений ТСПИ.

Параметрический канал утечки информации.

Технические каналы утечки информации при передаче ее по каналам связи.

Электрические линии связи.

Средства передачи электрических сигналов.

Каналы утечки информации за счет паразитных связей.

Опасные сигналы и их источники.

Электрические каналы утечки информации.

Контроль и прослушивание телефонных каналов связи

Электромагнитные каналы утечки информации.

Индукционный канал утечки информации.

Демаскирующие признаки радиоэлектронных средств.

Демаскирующие признаки объектов в видимом диапазоне электромагнитного спектра.

Демаскирующие признаки объектов в инфракрасном диапазоне электромагнитного спектра. Способы скрытого видеонаблюдения и съемки.

Тема 9. Пассивные средства защиты информации.

Методы и средства пассивной защиты.

Обеспечение безопасности мест хранения и обработки информации:

- автоматизированные контрольно-пропускные системы (в т.ч. с идентификацией личности) с использованием электромеханических запирающих и блокирующих устройств;
- системы защиты от НСД локальных и глобальных компьютерных сетей;
- автоматизированные системы контроля служебного документооборота (печати, архивации и пр.), электронной почты и т.п.

Защита линий связи и коммуникаций:

Нейтрализация каналов естественного (неумышленного) и искусственного (умышленного) хищения (разглашения) информации служащими.

Тема 10. Активные средства информационной защиты.

Методы и средства активной защиты:

- создание прицельных помех в канале утечки информации;
- снижение чувствительности (подавления или нейтрализация) датчиков каналов

утечки информации;

- кодирование сообщений;
- воздействия сильных электромагнитных, электрических, акустических, виброакустических и др. полей на каналы информационных хищений вне полосы частот информационных сигналов.

Тема 11. Принципы оценки эффективности систем инженерно-технической защиты информации.

Моделирование защиты информации. Модели системы защиты и показатели эффективности. Стоимость защиты. Рекомендации по выбору рациональных вариантов защиты информации и соответствующих технических средств.

Контроль эффективности мер по защите информации техническими средствами.

Технический контроль эффективности принимаемых мер защиты. Назначение, содержание, вид и методы технического контроля. Основные средства технического контроля.

Подготовка к практическим занятиям

Тема 1. Применение специальных технических средств перехвата сигналов связи и негласного получения (изменения, уничтожения) информации с технических средств ее хранения, обработки и передачи.

Тема 2. Оценка угроз перехвата информации, обрабатываемой ТСПИ по техническим каналам ПЭМИН.

Тема 3. Моделирование защиты информации. Методика составления модели угроз перехвата информации.

Тема 4. Разработка рекомендаций по выбору рациональных вариантов защиты информации и соответствующих технических средств.

Подготовка к лабораторной работе

Тема 1. Радиомониторинг объекта информатизации (ПЭВМ), выявление информативных частот ПЭМИН с помощью комплекса «Навигатор П3».

Тема 2. Ведение акустической разведки с помощью акустического и виброакустического преобразователей многофункционального прибора «Пиранья» и комплекса «Аврора-2».

Тема 3. Радиомониторинг объекта информатизации (ПЭВМ), выявление информативных частот ПЭМИН с помощью комплекса «Навигатор П3».

Тема 4. Оценка эффективности постановки активных электромагнитных помех от генератора шума низкочастотного Г2-59 с помощью индикатора поля и комплекса «Крона».

Тема 5. Использование приборов физического поиска специальных технических средств разведки.

Тема 6 Ведение акустической разведки с помощью акустического и виброакустического преобразователей многофункционального прибора «Пиранья» и комплекса «Аврора-2».

Тема 7. Оценка эффективности защиты речевой информации в телефонных линиях связи за счет использования прибора комплексной защиты от прослушивания «Прокруст-2000».

Тема 8. Контроль эффективности активных и пассивных средств защиты ПЭВМ комплексом «Навигатор П3».

5.1. Виды самостоятельной работы студентов

Таблица 5.1 – Виды самостоятельной работы студентов (СРС)

Номер темы (раздела) дисциплины	Вид самостоятельной работы студентов	Трудоёмкость, часов
1	2	3
1	Изучение теоретического материала	4
2	Подготовка к практическим занятиям	2
3	Подготовка к практическим занятиям	4
4	Подготовка к практическим занятиям Подготовка к лабораторной работе	2 4
5	Изучение теоретического материала	2
6	Изучение теоретического материала	2
7	Изучение теоретического материала Подготовка к лабораторной работе	4 4
8	Изучение теоретического материала Подготовка к практическим занятиям Подготовка к лабораторной работе	2 4 4
9	Изучение теоретического материала Подготовка к лабораторной работе	4 4
10	Изучение теоретического материала Подготовка к практическим занятиям	4 4
11	Изучение теоретического материала Подготовка к практическим занятиям Подготовка к лабораторной работе	2 2 4
	Итого: в **ч** / в **ЗЕ**	62 4

5.2. Индивидуальные задания (нет)

5.3 Образовательные технологии, используемые для формирования компетенций

Проведение лекционных занятий по дисциплине основывается на активном методе обучения, при которой учащиеся не пассивные слушатели, а активные участники занятия, отвечающие на вопросы преподавателя. Вопросы преподавателя нацелены на активизацию процессов усвоения материала. Преподаватель заранее намечает список вопросов, стимулирующих ассоциативное мышление и установления связей с ранее освоенным материалом. Проведение практических занятий основывается на интерактивной форме взаимодействия преподавателя и студентов между собой. Преподавателем предлагается проблема (ситуация, условия, ограничения, конкретный пример), и путем обсуждения находится решение. Место преподавателя в интерактивных занятиях сводится к направлению деятельности учащихся на достижение целей занятия. Проведение практических занятий основывается на активном применении технических средств и комплексов защиты информации, имеющихся в лаборатории кафедры АТ.

6 Фонд оценочных средств дисциплины

6.1 Текущий контроль освоения заданных дисциплинарных компетенций

Текущий контроль освоения дисциплинарных компетенций проводится в следующих формах:

- опрос, текущая контрольная работа для анализа усвоения материала предыдущей лекции;
- оценка работы студента на лекционных и практических занятиях в рамках рейтинговой системы.

6.2 Рубежный и промежуточный контроль освоения заданных дисциплинарных компетенций

Рубежный контроль освоения заданных компетенций проводится по результатам выполнения различных индивидуальных заданий по предусмотренным видам самостоятельной работы по дисциплине.

Средствами контроля являются индивидуальные задания на выполнение запланированных видов самостоятельной работы и формы представления результатов выполненной работы.

Объектами рубежного контроля являются компоненты заявленных дисциплинарных компетенций.

6.3 Итоговый контроль освоения заданных дисциплинарных компетенций

1) **Зачёт** *«Не предусмотрен»*

2) **Экзамен**

Экзамен по дисциплине проводится устно по билетам. Билет содержит два теоретических вопроса и одно практическое задание.

Экзаменационная оценка выставляется с учётом результатов рубежной аттестации.

Фонды оценочных средств, включающие типовые задания, контрольные работы, тесты и методы оценки, критерии оценивания, перечень контрольных точек и таблица планирования результатов обучения, позволяющие оценить результаты освоения данной дисциплины, включены в состав УМКД.

6.4 Виды текущего, рубежного и итогового контроля освоения элементов и частей компетенций

Таблица 6.4 - Виды контроля освоения элементов и частей компетенций

Контролируемые результаты освоения дисциплины (ЗУВы)	Вид контроля					
	ТТ	РТ	КР	ГР (КР)	Трен.	Экзамен
В результате освоения частей компетенции студент **знает**: Принципы и методы организационной защиты информации. Технические каналы утечки информации. Возможности технических разведок. Способы и средства защиты информации от утечек по техническим каналам.	X		X		X	X
умеет: Анализировать и оценивать угрозы информационной безопасности объекта. Пользоваться нормативными документами по защите информации.	X		X		X	
владеет: Методами и средствами выявления угроз безопасности автоматизированным системам. Методами технической защиты информации. Методами формирования требований по защите информации. Методами расчета и инструментального контроля показателей технической защиты информации.	X		X		X	

ТТ – текущее тестирование (контроль знаний по теме);

РТ – рубежное тестирование по модулю (автоматизированная система контроля знаний);

КР – рубежная контрольная работа по модулю (оценка умений);

ГР (КР) – индивидуальные графические или курсовые работы (оценка умений и владений);

Трен. (ЛР) – выполнение тренажей и лабораторных работ с подготовкой отчёта (оценка владения).

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**		**Р3**		**Р4**						**Р5**					
Лекции	1	2	2	2	2	2	2	2		2				2	2	2	1		**24**
Практические занятия				2					2									4	**8**
Семинары																			
Лабораторные работы			2	2	4						4		4		2		2		**20**
КСР													1					1	**2**
Подготовка к практическим занятиям		2		2	4						2	2				2	2	2	**18**
Изучение теоретического материала	1	1	2			2	2	2	2	2				2	2	2	2	2	**24**
Подготовка к лабораторным работам				2	2						4	2	2	2	2	2	2		**20**
Модуль:	**М1**							**М2**						**М3**					
Контр. тестирование							+											+	2
Дисциплин. Контроль (Экзамен)																			**36**

8 Учебно-методическое и информационное обеспечение дисциплины

8.1 Карта обеспеченности дисциплины учебно-методической литературой

Б1.Б.29 Техническая защита информации	Блок 1 (*цикл дисциплины*)
(*полное название дисциплины*)	[x] обязательная / [ ] 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: [x] специалист / [ ] бакалавр / [ ] магистр	Форма обучения: [x] очная / [ ] заочная / [ ] очно-заочная
(*аббревиатура направления / специальности*)		

_____2017_____ (*год утверждения учебного плана ООП*)	Семестр(ы) 7	Количество групп 1; Количество студентов 20

Костецкий Валерий Павлович, доцент
электротехнический факультет,
кафедра АТ, телефон: 239-17-86.

СПИСОК ИЗДАНИЙ

№	Библиографическое описание (автор, заглавие, вид издания, место, издательство, год издания, количество страниц)	Количество экземпляров в библиотеке
1	2	3
	1 Основная литература	
1	Зайцев, А.П. Технические средства и методы защиты информации : учебник / Р.В. Мещеряков, А.А. Шелупанов, А.П. Зайцев, 7-е изд., испр., М, Горячая линия – Телеком, 2012, 443 с.	21
2	В.П. Мельников, Защита информации, учебник, М, «Академия», 2014, 304 стр.	6
3	Бузов, Калинин, Кондратьев, Защита от утечки информации по техническим каналам, учебное пособие, М, изд. «Горячая линия-Телеком», 2005, 414 стр.	20
3	А.А. Торокин, Инженерно-техническая защита информации, учебное пособие, М, Гелиос АРВ, 2005, 959 стр.	12
	2 Дополнительная литература	
	2.1 Учебные и научные издания	
1	А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин, Защита информации, учебное пособие -2 изд. М, РИОР ИНФРА-М, 2015, 392 с.	5
2	А.П. Зайцев, А.А. Шелупанов, Справочник по техническим средствам защиты информации и контроля технических каналов утечки информации, учебное пособие, Томск: ТГУСУ и Р, 2004, 204 стр.	5
3	А.П. Зайцев, А.А. Шелупанов, Технические средства обеспечения информационной безопасности, учебное пособие, ч. 2, Томск: ТМЦДО, 2004, 279 стр.	5
4	Меньшаков Ю.К., Защита объектов и информации от технических средств разведки, учебное пособие, М, Изд-во РГГУ, 2002, 399 стр.	25
	2.2 Периодические издания	
1	Безопасность информационных технологий, журнал, изд. МИФИ, с 1994	
	2.3 Нормативно-технические издания	
	2.4 Официальные издания	
	2.5 Перечень ресурсов информационно-телекоммуникационной сети, необходимых для освоения дисциплины	
1.	Электронная библиотека Научной библиотеки Пермского национального исследовательского политехнического университета [Электронный ресурс] : [полнотекстовая база данных электронных документов, изданных в Издательстве ПНИПУ] / Перм. нац. исслед. политехн. ун-т, Науч. б-ка. – Пермь, 2016. – Режим доступа: http://elib.pstu.ru, свободный. – Загл. с экрана.	

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.	Электронно-библиотечная система Библиокомплектатор [Электронный ресурс] : [платформа и полнотекстовая база данных : электрон. версии кн., журн. по гуманит., обществ., естеств. и техн. наукам] / Ай Пи Эр Медиа, Ай Пи Ар Букс. – [Саратов, 2016]. – Режим доступа: http://www.bibliocomplectator.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

Карта книго-обеспеченности в библиотеку сдана

8.2 Компьютерные обучающие и контролирующие программы

Таблица 8.2 – Программы, используемые для обучения и контроля

№ п.п.	Вид учебного занятия	Наименование программного продукта	Рег. номер	Назначение
1	2	3	4	5
1	ПЗ	Специальное программное обеспечение «Филин»	1627	Поиск радиоизлучающих устройств
2	ПЗ	Специальное программное обеспечение «Аврора-2»	Инв. 4885665	Формирование и излучение в эфир радиосигналов, имитирующих работу основных типов радиопередающих устройств.
3	ПЗ	Специальное программное обеспечение «Улан-2»	U-0111 Инв. 0485665	Обнаружение фактов несанкционированного доступа в проводных коммуникациях.
4	ПЗ	Специальное программное обеспечение «Навигатор ПЗ»	468166.323 ПО 19248 usb	Для автоматического, автоматизированного и экспертного поиска сигналов ПЭМИН от проверяемых технических средств, измерения частоты и пикового значения амплитуды найденных сигналов, хранения, обработки и представления результатов поиска и измерений в удобном для оператора виде, и применяется на объектах сферы обороны и безопасности.

8.3 Аудио- и видео-пособия

Таблица 8.3 – Используемые аудио- и видео-пособия

Вид аудио-, видео-пособия				Наименование учебного пособия
теле-фильм	кино-фильм	слайды	аудио-пособие	
1	2	3	4	5
		+		Презентации с материалами лекций по дисциплине в формате PowerPoint.
+				Обучающий тренажерный комплекс «Заря»

9 Материально-техническое обеспечение дисциплины

9.1 Специализированные лаборатории и классы

Таблица 9.1 – Специализированные лаборатории и классы

№ п.п.	Помещения			Площадь, $м^2$	Количество посадочных мест
	Название	Принадлежность (кафедра)	Номер аудитории		
1	2	3	4	5	6
1	Лаборатория КЗИ	Кафедра АТ	308	30	18

9.2 Основное учебное оборудование

Таблица 9.2 – Учебное оборудование

№ п.п.	Наименование и марка оборудования (стенда, макета, плаката)	Кол-во, ед.	Форма приобретения / владения (собственность, оперативное управление, аренда и т.п.)	Номер аудитории
1	2	3	4	5
1	Селективный микровольтметр SMV 8.5	1	Оперативное управление	308
2	Селективный микровольтметр SMV 11	1		
3	Детектор поля ST 006	2		
4	Фильтр сетевой помехоподавляющий	2		
5	Генератор шума низкочастотный Г2-59	1		
6	Генератор GFG-8216A	2		
7	Комплекс обнаружения радиоизлучающих	1		
8	Модуль защиты телефонной линии	1		
9	Многофункциональный поисковый прибор ST 031	1		
10	Индикатор состояния телефонных линий SEC-	1		
11	Устройство визуального контроля «Шмель»	1		
12	Комплекс имитации радиопередающих	1		
13	Комплекс измерений ПЭМИН «Навигатор П3»	1		
14	Комплекс обнаружения фактов	1		

Лист регистрации изменений

№ п.п.	Содержание изменения	Дата, номер протокола заседания кафедры. Подпись заведующего кафедрой
1	2	3
1		
2		
3		
4		