Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение высшего образования

Пермский национальный исследовательский политехнический университет

УТВЕРЖДАЮ
Проректор по образовательной деятельности

_____ А.Б. Петроченков

« 18 » июля 20 23 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Дисциплина: Техническая защита информации
(наименование)

Форма обучения: очная
(очная/очно-заочная/заочная)

Уровень высшего образования: специалитет
(бакалавриат/специалитет/магистратура)

Общая трудоёмкость: 144 (4)
(часы (ЗЕ))

Направление подготовки: 10.05.03 Информационная безопасность автоматизированных систем
(код и наименование направления)

Направленность: Безопасность открытых информационных систем (СУОС)
(наименование образовательной программы)

Пермь 2023

1. Общие положения

1.1. Цели и задачи дисциплины

Целью освоения дисциплины «Техническая защита информации»является формирование у студентов навыков, необходимых для решения следующих профессиональных задач:

1. Разработка проектов систем и подсистем управления информационной безопасностью объекта в соответствии с техническим заданием;
2. Проведение инструментального мониторинга защищенности объекта;
3. Поиск рациональных решений при разработке средств защиты информации с учетом требований качества, надежности и стоимости, а также сроков исполнения;
4. Установка, настройка, эксплуатация и обслуживание аппаратно-программных средств защиты информации;
5. Обеспечение эффективного функционирования средств защиты информации с учетом требований по обеспечению защищенности компьютерной системы.

1.2. Изучаемые объекты дисциплины

Объекты информатизации, включая компьютерные, автоматизированные, телекоммуникационные, информационные ресурсы и информационные ресурсы в условиях существования угроз в информационной сфере. Технологии обеспечения информационной безопасности объектов различного уровня, которые связаны с информационными технологиями, используемыми на этих объектах. Процессы управления информационной безопасностью защищаемых объектов.

1.3. Входные требования

Не предусмотрены

2. Планируемые результаты обучения по дисциплине

Компетенция	Индекс индикатора	Планируемые результаты обучения по дисциплине (знать, уметь, владеть)	Индикатор достижения компетенции, с которым соотнесены планируемые результаты обучения	Средства оценки
ОПК-15	ИД-1ОПК-15	Знает основные угрозы безопасности информации, основанные на утечке информации по техническим каналам	Знает основные угрозы безопасности информации и модели нарушителя в автоматизированных системах; содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и систем защиты информации;	Отчёт по практическому занятию

Компетенция	Индекс индикатора	Планируемые результаты обучения по дисциплине (знать, уметь, владеть)	Индикатор достижения компетенции, с которым соотнесены планируемые результаты обучения	Средства оценки
ОПК-15	ИД-2ОПК-15	Умеет выстраивать правильный алгоритм действий по созданию автоматизированного рабочего места в соответствии с требованиями защиты от утечек по техническим каналам	Умеет контролировать события безопасности и действия пользователей автоматизированных систем; документировать процедуры и результаты контроля функционирования системы защиты информации автоматизированной системы; анализировать программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей безопасности информации в автоматизированных системах	Отчёт по практическому занятию
ОПК-15	ИД-3ОПК-15	Владеет навыками оценки защищённости объекта информатизации от утечек информации по техническим каналам с помощью инструментальных методов	Владеет навыками контроля эффективность принятых мер по реализации политик безопасности информации автоматизированных систем	Отчёт по практическому занятию
ОПК-9	ИД-1ОПК-9	Знает требования к рабочему месту сотрудника, обеспечивающие безопасность обработки конфиденциальной информации	Знает основные характеристики сигналов электросвязи, спектры и виды модуляции; способы кодирования информации; основные задачи и понятия криптографии; модели шифров и математические методы их исследования; технические средства защиты информации	Отчёт по практическому занятию
ОПК-9	ИД-2ОПК-9	Умеет на основе полученных аппаратурным методом данных выносить решение о состоянии защищённости объекта информатизации	Умеет анализировать основные характеристики и возможности телекоммуникационных систем; применять математические методы исследования моделей шифров; использовать типовые	Отчёт по практическому занятию

Компетенция	Индекс индикатора	Планируемые результаты обучения по дисциплине (знать, уметь, владеть)	Индикатор достижения компетенции, с которым соотнесены планируемые результаты обучения	Средства оценки
			криптографические алгоритмы и технические средства защиты информации;	
ОПК-9	ИД-3ОПК-9	Владеет методами и средствами оценки уровня защищённости объекта от утечки информации по техническим каналам	Владеет методами и средствами технической защиты информации	Отчёт по практическому занятию

3. Объем и виды учебной работы

Вид учебной работы	Всего часов	Распределение по семестрам в часах
		Номер семестра
		7
1. Проведение учебных занятий (включая проведение текущего контроля успеваемости) в форме: 1.1. Контактная аудиторная работа, из них:	54	54
- лекции (Л)	24	24
- лабораторные работы (ЛР)		
- практические занятия, семинары и (или) другие виды занятий семинарского типа (ПЗ)	28	28
- контроль самостоятельной работы (КСР)	2	2
- контрольная работа		
1.2. Самостоятельная работа студентов (СРС)	54	54
2. Промежуточная аттестация		
Экзамен	36	36
Дифференцированный зачет		
Зачет		
Курсовой проект (КП)		
Курсовая работа (КР)		
Общая трудоемкость дисциплины	144	144

4. Содержание дисциплины

Наименование разделов дисциплины с кратким содержанием	Объем аудиторных занятий по видам в часах			Объем внеаудиторных занятий по видам в часах
	Л	ЛР	ПЗ	СРС
7-й семестр				

Наименование разделов дисциплины с кратким содержанием	Объем аудиторных занятий по видам в часах			Объем внеаудиторных занятий по видам в часах
	Л	ЛР	ПЗ	СРС
Технические каналы утечки информации	20	0	26	14
1. Оптическая разведка; 2. Оптикоэлектронная разведка; 3. Радиоэлектронная разведка; 4. Гидроакустическая разведка; 5. Акустическая разведка; 6. Радиационная разведка; 7. Химическая разведка; 8. Сейсмическая разведка; 9. Магнитометрическая разведка; 10. Компьютерная разведка.				
Особенности ведения современной технической разведки	4	0	2	40
1. Демаскирующие признаки 2. Разведка на основе открытых источников 3. Промышленный шпионаж				
ИТОГО по 7-му семестру	24	0	28	54
ИТОГО по дисциплине	24	0	28	54

Тематика примерных практических занятий

№ п.п.	Наименование темы практического (семинарского) занятия
1	Разработка методических рекомендаций по защите рабочего места сотрудника
2	Создание паспорта объекта информатизации (по техническим каналам утечки информации)

5. Организационно-педагогические условия

5.1. Образовательные технологии, используемые для формирования компетенций

Проведение лекционных занятий по дисциплине основывается на активном методе обучения, при котором учащиеся не пассивные слушатели, а активные участники занятия, отвечающие на вопросы преподавателя. Вопросы преподавателя нацелены на активизацию процессов усвоения материала, а также на развитие логического мышления. Преподаватель заранее намечает список вопросов, стимулирующих ассоциативное мышление и установление связей с ранее освоенным материалом.

Практические занятия проводятся на основе реализации метода обучения действием: определяются проблемные области, формируются группы. При проведении практических занятий преследуются следующие цели: применение знаний отдельных дисциплин и креативных методов для решения проблем и приятия решений; отработка у обучающихся навыков командной работы, межличностных коммуникаций и развитие лидерских качеств; закрепление основ теоретических знаний.

При проведении учебных занятий используются интерактивные лекции, групповые дискуссии, ролевые игры, тренинги и анализ ситуаций и имитационных моделей.

5.2. 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 и индивидуальным комплексным заданиям на самостоятельную работу.

4. 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.

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

6.1. Печатная учебно-методическая литература

№ п/п	Библиографическое описание (автор, заглавие, вид издания, место, издательство, год издания, количество страниц)	Количество экземпляров в библиотеке
1. Основная литература		
1	Данилов А. Н. Инженерно-техническая защита информации : учебное пособие / А. Н. Данилов, А. Л. Лобков. - Пермь: Изд-во ПГТУ, 2007.	69
2	Рагозин Ю. Н. Инженерно-техническая защита информации : учебное пособие / Ю. Н. Рагозин. - Санкт-Петербург: ИЦ Интермедия, 2018.	4
2. Дополнительная литература		
2.1. Учебные и научные издания		
1	Технические средства защиты информации. - Киев: , ООО ТИД ДС, 2003. - (Информационная безопасность офиса; Вып. 1).	1
2	Технические средства и методы защиты информации : учебное пособие для вузов / А. П. Зайцев [и др.]. - Москва: Горячая линия-Телеком, 2009.	21
2.2. Периодические издания		
	Не используется	
2.3. Нормативно-технические издания		
	Не используется	
3. Методические указания для студентов по освоению дисциплины		
	Не используется	
4. Учебно-методическое обеспечение самостоятельной работы студента		
	Не используется	

6.2. Электронная учебно-методическая литература

Вид литературы	Наименование разработки	Ссылка на информационный ресурс	Доступность (сеть Интернет / локальная сеть; авторизованный / свободный доступ)
Дополнительная литература	Титов А. А. Инженерно-техническая защита информации / Титов А. А. - Москва: ТУСУР, 2010.	http://elib.pstu.ru/Record/lan4959	сеть Интернет; авторизованный доступ
Методические указания для студентов по освоению дисциплины	Круглов Р. С. Обнаружение радиопередающих закладных устройств детектором СВЧ-поля и металлодетектором / Круглов Р. С. - Москва: ТУСУР, 2008.	http://elib.pstu.ru/Record/lan11409	сеть Интернет; авторизованный доступ
Основная литература	Исаева М. Ф. Техническая защита информации / Исаева М. Ф. - Санкт-Петербург: ПГУПС, 2017.	http://elib.pstu.ru/Record/lanRU-LAN-BOOK-101600	сеть Интернет; авторизованный доступ

6.3. Лицензионное и свободно распространяемое программное обеспечение, используемое при осуществлении образовательного процесса по дисциплине

Вид ПО	Наименование ПО
Операционные системы	Windows 10 (подп. Azure Dev Tools for Teaching)
Офисные приложения.	Adobe Acrobat Reader DC. бесплатное ПО просмотра PDF
Офисные приложения.	LibreOffice 6.2.4. OpenSource, бесплатен.
Прикладное программное обеспечение общего назначения	Dr.Web Enterprise Security Suite, 3000 лиц, ПНИПУ ОЦНИТ 2017

6.4. Современные профессиональные базы данных и информационные справочные системы, используемые при осуществлении образовательного процесса по дисциплине

Наименование	Ссылка на информационный ресурс
Научная библиотека Пермского национального исследовательского политехнического университета	http://lib.pstu.ru/
Электронно-библиотечеая система Лань	https://e.lanbook.com/
Электронно-библиотечная система IPRbooks	http://www.iprbookshop.ru/
Информационные ресурсы Сети КонсультантПлюс	http://www.consultant.ru/
База данных компании EBSCO	https://www.ebsco.com/

7. Материально-техническое обеспечение образовательного процесса по дисциплине

Вид занятий	Наименование необходимого основного оборудования и технических средств обучения	Количество единиц
Лекция	Проектор	1
Практическое занятие	Персональный компьютер IBM PC	12

8. Фонд оценочных средств дисциплины

Описан в отдельном документе

Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение высшего образования
«Пермский национальный исследовательский политехнический университет»

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ
для проведения промежуточной аттестации обучающихся по дисциплине «Техническая защита информации»
Приложение к рабочей программе дисциплины

Специальность:	10.05.03 Информационная безопасность автоматизированных систем
Специализация (профиль) образовательной программы:	Безопасность открытых информационных систем
Квалификация выпускника:	Специалист
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.

Форма промежуточной аттестации:
Экзамен: 7 семестр

Пермь 2023

Фонд оценочных средств для проведения промежуточной аттестации обучающихся для проведения промежуточной аттестации обучающихся по дисциплине является частью (приложением) к рабочей программе дисциплины. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине разработан в соответствии с общей частью фонда оценочных средств для проведения промежуточной аттестации основной образовательной программы, которая устанавливает систему оценивания результатов промежуточной аттестации и критерии выставления оценок**.** Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине устанавливает формы и процедуры текущего контроля успеваемости и промежуточной аттестации обучающихся по дисциплине.

1. Перечень контролируемых результатов обучения по дисциплине, объекты оценивания и виды контроля

Согласно РПД, освоение учебного материала дисциплины запланировано в течение одного семестра (7-го семестра учебного плана) и разбито на 3 учебных модуля. В каждом модуле предусмотрены аудиторные лекционные и практические занятия, а также самостоятельная работа студентов. В рамках освоения учебного материала дисциплины формируется компоненты компетенций *знать, уметь, владеть*, указанные в РПД, которые выступают в качестве контролируемых результатов обучения по дисциплине (табл. 1.1).

Контроль уровня усвоенных знаний, освоенных умений и приобретенных владений осуществляется в рамках текущего, рубежного и промежуточного контроля при изучении теоретического материала, сдаче отчетов по практическим заданиям и экзамена. Виды контроля сведены в таблицу 1.1.

Таблица 1.1. Перечень контролируемых результатов обучения по дисциплине

Контролируемые результаты обучения по дисциплине (ЗУВы)	**Вид контроля**					
	Текущий		**Рубежный**		**Итоговый**	
	С	**ТО**	**ПЗ**	**Т/КР**	**СРС**	**Экзамен**
Усвоенные знания						
З.1 Знать требования к рабочему месту сотрудника, обеспечивающие безопасность обработки конфиденциальной информации, принципы формирования политики информационной безопасности в автоматизированных системах.		ТО1	ПЗ1	Т	ОПР	ТВ
Освоенные умения						
У.1 уметь классифицировать и оценивать угрозы информационной безопасности, выстраивать правильный алгоритм действий по созданию автоматизированного рабочего места в соответствии с требованиями защиты от утечек по техническим каналам.			ПЗ 2 ПЗ 3	Т	ОПР	ПЗ
Приобретенные владения						
В.1 владеть навыками использования источников профессиональной терминологии в области информационной безопасности и защиты информации, оценки защищённости объекта информатизации от утечек информации по техническим каналам с помощью инструментальных методов			ПЗ 4 ПЗ 5 ПЗ 6 ПЗ 7	Т	ОПР	КЗ

С – собеседование по теме; ТО – коллоквиум (теоретический опрос); КЗ – кейс-задача (индивидуальное задание); ОЛР – отчет по лабораторной работе; ОПР – отчет по практической работе, Т/КР – рубежное тестирование (контрольная работа, курсовая работа); ТВ – теоретический вопрос; ПЗ – практическое задание; КЗ – комплексное задание экзамена.

Итоговой оценкой достижения результатов обучения по дисциплине является промежуточная аттестация в виде экзамена, проводимая с учетом результатов текущего и рубежного контроля.

2. Виды контроля, типовые контрольные задания и шкалы оценивания результатов обучения

Текущий контроль успеваемости имеет целью обеспечение максимальной эффективности учебного процесса, управление процессом формирования заданных компетенций обучаемых, повышение мотивации к учебе и предусматривает оценивание хода освоения дисциплины. В соответствии с Положением о проведении текущего контроля успеваемости и промежуточной аттестации обучающихся по образовательным программам высшего образования – программам бакалавриата, специалитета и магистратуры в ПНИПУ предусмотрены следующие виды и периодичность текущего контроля успеваемости обучающихся:

- входной контроль, проверка исходного уровня подготовленности обучаемого и его соответствия предъявляемым требованиям для изучения данной дисциплины;
- текущий контроль усвоения материала (уровня освоения компонента «знать» заданных компетенций) на каждом групповом занятии и контроль посещаемости лекционных занятий;
- промежуточный и рубежный контроль освоения обучаемыми отдельных компонентов «знать», «уметь» заданных компетенций путем компьютерного или бланочного тестирования, контрольных опросов, контрольных работ (индивидуальных домашних заданий), защиты отчетов по лабораторным работам, рефератов, эссе и т.д.

Рубежный контроль по дисциплине проводится на следующей неделе после прохождения модуля дисциплины, а промежуточный – во время каждого контрольного мероприятия внутри модулей дисциплины;

- межсессионная аттестация, единовременное подведение итогов текущей успеваемости не менее одного раза в семестр по всем дисциплинам для каждого направления подготовки (специальности), курса, группы;
- контроль остаточных знаний.

2.1. Текущий контроль усвоения материала

Текущий контроль усвоения материала в форме собеседования или выборочного теоретического опроса в рамках контроля самостоятельной работы студентов проводится по каждой теме. Результаты по 4-балльной шкале оценивания заносятся в журнал преподавателя и учитываются в виде интегральной оценки при проведении промежуточной аттестации.

Вопросы для самостоятельного изучения:

Тема 1. Оптическая разведка.

Тема 2. Оптикоэлектронная разведка.

Тема 3. Радиоэлектронная разведка.

Тема 4. Гидроакустическая разведка.
Тема 5. Акустическая разведка.
Тема 6. Радиационная разведка.
Тема 7. Химическая разведка.
Тема 8. Сейсмическая разведка.
Тема 9. Магнитометрическая разведка.
Тема 10. Компьютерная разведка.
Тема 11. Особенности ведения современной технической разведки:
- Демаскирующие признаки;
- Разведка на основе открытых источников;
- Промышленный шпионаж.

2.2. Рубежный контроль

Рубежный контроль для комплексного оценивания усвоенных знаний, освоенных умений и приобретенных владений (табл. 1.1) проводится в форме отчета по результатам практических заданий (после изучения каждого модуля учебной дисциплины).

Всего запланировано 8 практических занятий. Темы практических занятий приведены в РПД.

Отчет по выполнению практического задания проводится индивидуально каждым студентом. Типовые шкала и критерии оценки приведены в общей части ФОС образовательной программы.

2.3. Промежуточная аттестация (итоговый контроль)

Допуск к промежуточной аттестации осуществляется по результатам текущего и рубежного контроля. Условиями допуска являются успешная сдача всех лабораторных работ и положительная интегральная оценка по результатам текущего и рубежного контроля.

Промежуточная аттестация, согласно РПД, проводится в виде экзамена по дисциплине устно по билетам. Билет содержит теоретические вопросы (ТВ) для проверки усвоенных знаний и практические задания (ПЗ) для проверки освоенных умений всех заявленных компетенций.

Билет формируется таким образом, чтобы в него попали вопросы и практические задания, контролирующие уровень сформированности ***всех*** заявленных компетенций. Форма билета представлена в общей части ФОС образовательной программы.

2.3.1. Типовые вопросы и задания для экзамена по дисциплине

Типовые вопросы для контроля усвоенных знаний:

1. Цели и задачи технической разведки. Классификация, принципы организации и ведения технической разведки;
2. Оптическая разведка (понятие, цели и задачи). Виды оптической разведки (визуально-оптическая, фотографическая). Основные элементы и характеристики канала утечки информации;

3. Оптико-электронная разведка (понятие, цели и задачи, классификация). Виды оптико-электронной разведки (телевизионная, инфракрасная, лазерная);

4. Радиоэлектронная разведка (понятие, цели и задачи, классификация, отличие от оптико-электронной разведки);

5. Радио - и радиотехническая разведка (понятие, цели и задачи, структурная типовая схема станции РР и РТР);

6. Радиолокационная разведка (понятие, задачи, виды РЛС, характеристики аппаратуры РЛР, преимущества радиолокационного наблюдения);

7. Параметрическая радиолокационная разведка (понятие, цели и задачи, применяемые методы измерения расстояний до объектов, блок-схема радиолокационной станции с общей приемопередающей антенной);

8. Радиотепловая разведка (понятие, цели и задачи, особенности приема радиотепловых сигналов, принцип действия радиометра и теплолокатора);

9. Разведка побочных электромагнитных излучений и наводок (понятие ПЭМИН и физические явления, лежащие в основе появления различных каналов утечки информации, КУИ при эксплуатации основных ТСПИ и ВТСС);

10. Акустические преобразователи информационных сигналов (индуктивные датчики, пьезоэлектрические датчики, оптические преобразователи, излучатели электромагнитных колебаний);

11. Паразитные связи и наводки. Средства разведки ПЭМИН;

12. Способы несанкционированного подключения к информационным телефонным линиям (подключение к телефонной линии с помощью согласующего устройства, с компенсацией напряжения, индукционного датчика);

13. Гидроакустическая разведка (понятие, цели и задачи, характеристики аппаратуры). Гидроакустические средства разведки и наблюдения;

14. Акустическая разведка (понятие, задачи, возможные каналы утечки информации). Виды акустических разведывательных приборов;

15. Закладные устройства перехвата акустической (речевой) информации (понятие, классификация, характеристики);

16. Радиационная разведка (понятие, цели и задачи). Явление радиоактивности. Свойства радиоактивных излучений.

17. Основные характеристики радиоактивных излучений и единицы их измерения. Приборы для измерения ионизирующих излучений;

18. Химическая разведка (понятие, цели и задачи). Методы, средства измерения и виды аппаратуры химической разведки;

19. Сейсмическая разведка (назначение, задачи). Основные особенности распространения волн в упругих средах и методы их исследования;

20. Магнитометрическая разведка (назначение, задачи). Основные характеристики магнитного поля. Методы измерений элементов земного магнетизма и аппаратура ММР;

21. Компьютерная разведка (понятие, цели и задачи). Структурная схема.

22. Основные способы несанкционированного доступа к автоматизированной системе обработки данных (преодоление СЗИ, парольной защиты, использование программных закладок и компьютерных вирусов);

23. Особенности ведения современной технической разведки. Разведка на основе открытых источников (OSINT), промышленный шпионаж.

Типовые практические задания для контроля освоенных умений:

1. Руководствуясь инструкцией по эксплуатации ST031 «Пиранья», подготовить прибор к работе, произвести проверку его работоспособности, настройку и юстировку. Зафиксировать характеристики тестовых сигналов, излучаемых КУИ.

2. Обнаружить при помощи прибора ST031 «Пиранья» источник излучения на объекте информатизации, вызванные несанкционированным подключением, для чего:

- подготовить прибор ST031 «Пиранья» к работе;
- произвести проверку его работоспособности и настройку;
- провести обследование помещения прибором ST031 «Пиранья» в одном из режимов, при обнаружении посторонних сигналов провести их идентификацию и определить характеристики. По возможности установить источник этих излучений и его примерное местоположение.
- сделать необходимые выводы.

3. Руководствуясь инструкцией по эксплуатации «Навигатор П3» подготовить прибор к работе, произвести проверку его работоспособности, настройку и юстировку.

4. Выявить информативные частоты ПЭМИН настольного компьютера с помощью измерительный комплекса ПЭМИН «Навигатор П3» в одной контрольной точке измерений, для чего:

- подготовить измерительные антенны к работе, установить измерительные антенны напротив исследуемого технического средства и подключить их к измерительному прибору;
- включить измерительное оборудование и проверить его работоспособность в ручном режиме;
- подготовить исследуемое техническое средство к запуску тестового режима работы;
- запустить поисковую и измерительную программу «Navigat.exe», выбрать используемое оборудование и интерфейс управления прибором;
- с помощью одного из методов обнаружения сигналов сформировать список сигналов ПЭМИН тестируемого оборудования;
- сохранить результаты обнаружения сигналов в файле или в отчете поиска сигналов ПЭМИН с отметкой «Найденные сигналы»;
- сделать необходимые выводы.

5. Руководствуясь инструкцией по эксплуатации «Анализатор спектра» NS-30 подготовить прибор к работе, произвести проверку его работоспособности, настройку и юстировку.

6. Выявить информативные частоты ПЭМИН на объекте информатизации с помощью измерительного комплекса NS-30 «Анализатор спектра» для чего:

- подготовить измерительные антенны к работе, установить на штатив и подключить их к измерительному прибору;
- включить измерительное оборудование произвести проверку его работоспособности, настройку и юстировку;
- запустить поисковую и измерительную программу;
- сформировать список обнаруженных сигналов ПЭМИН, продемонстрировать выявленные информационные частоты;
- сделать необходимые выводы.

7. Руководствуясь инструкцией по эксплуатации комплекса обнаружения радиоизлучающих устройств «Крона» подготовить прибор к работе, произвести проверку его работоспособности, настройку и произвести мониторинг на наличие радиоизлучающих устройств.

8. Обнаружить излучение сигнала, передающего данные по радиоканалу и провести мониторинг электромагнитной обстановки в контролируемом помещении. Определить частные характеристики данного сигнала с помощью аппаратуры «Крона», для чего:
- подготовить к работе аппаратуру «Крона» в соответствии с инструкцией по эксплуатации;
- подключить измерительную антенну;
- подключить и настроить ВЧ-тюнер;
- произвести настройку аппаратуры «Крона» для осуществления поиска сигнала в радиочастотном диапазоне;
- произвести поиск сигналов в радиочастотном диапазоне и мониторинг электромагнитной обстановки;
- определить частные характеристики обнаруженных сигналов;
- сделать необходимые выводы.

9. Обнаружить излучение сигнала имитатора закладочного устройства, сгенерированного с помощью комплекса «Аврора-2» и определить частные характеристики данного сигнала с помощью аппаратуры «Крона», для чего:
- произвести настройку имитатора сигналов (комплекс «Аврора-2») для излучения тестового сигнала ЧМ мкф на частоте 650 МГц.
- подготовить к работе аппаратуру «Крона» в соответствии с инструкцией по эксплуатации;
- произвести настройку аппаратуры «Крона» для осуществления поиска тестового сигнала от имитатора комплекс «Аврора-2» в диапазоне 500 МГц – 700 МГц;
- произвести поиск и обнаружение тестового сигнала;
- запустить аппаратуру «Крона» в режим локализации тестового сигнала
- обнаружить излучение сигнала имитатора закладочного устройства;
- сделать необходимые выводы.

10. Обнаружить при помощи аппаратуры «Улан -2» изменения характеристик линии (кабеля) на объекте информатизации, вызванные несанкционированным подключением, для чего:

- подготовить аппаратуру «Улан -2» к работе;
- подключить к измерительной колодке проверяемую линию (кабель):
- создать запись о новой линии;
- произвести измерения проверяемой линии (напряжения постоянного тока, сопротивления, емкости и индуктивности);
- вывести на дисплей вольтамперную, импульсную переходную и амплитудно-частотную характеристику, параметрическую зависимость выходного тока от входного гармонического напряжения (фигура Лиссажу), импульсную рефлектограмму проверяемой линии;
- сделать необходимые выводы.

2.3.2. Шкалы оценивания результатов обучения на экзамене

Оценка результатов обучения по дисциплине в форме уровня сформированности компонентов *знать, уметь, владеть* заявленных компетенций проводится по 5 балльной шкале оценивания путем выборочного контроля во время экзамена.

Типовые шкала и критерии оценки результатов обучения при сдаче экзамена для компонентов *знать, уметь и владеть* приведены в общей части ФОС образовательной программы.

3. Критерии оценивания уровня сформированности компонентов и компетенций

3.1. Оценка уровня сформированности компонентов компетенций

При оценке уровня сформированности компетенций в рамках выборочного контроля при экзамене считается, что *полученная оценка за компонент проверяемой в билете компетенции обобщается на соответствующий компонент всех компетенций, формируемых в рамках данной учебной дисциплины*.

Типовые критерии и шкалы оценивания уровня сформированности компонентов компетенций приведены в общей части ФОС образовательной программы.

3.2. Оценка уровня сформированности компетенций

Общая оценка уровня сформированности всех компетенций проводится путем агрегирования оценок, полученных студентом за каждый компонент формируемых компетенций, с учетом результатов текущего и рубежного контроля в виде интегральной оценки по 5 балльной шкале. Все результаты контроля заносятся в оценочный лист и заполняются преподавателем по итогам промежуточной аттестации.

Форма оценочного листа и требования к его заполнению приведены в общей части ФОС образовательной программы.

При формировании итоговой оценки промежуточной аттестации в виде экзамена используются типовые критерии, приведенные в общей части ФОС образовательной программы.