МИНОБРНАУКИ РОССИИ
федеральное государственное бюджетное образовательное учреждение
высшего образования
«ИРКУТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
ФГБОУ ВО «ИГУ»
Кафедра радиофизики и радиоэлектроники

УТВЕРЖДАЮ
Декан _____ Буднев Н.М.
«22» апреля 2020 г.

Рабочая программа дисциплины

Наименование дисциплины **__Б1.Б.09 Техническая защиты информации**

Направление подготовки 10.03.01 Информационная безопасность

Направленность (профиль) подготовки №7 «Техническая защита информации»

Квалификация выпускника бакалавр

Форма обучения очная

Согласовано с УМК физического факультета

Протокол № 25 от «21» апреля 2020 г.
Председатель _____ Буднев Н.М.

Рекомендовано кафедрой радиофизики и радиоэлектроники:

Протокол № 8
От «20» марта 2020 г.
И.О.Зав. кафедрой _____ Колесник С.Н.

Иркутск 2020 г.

Содержание

стр.

1. Цели и задачи дисциплины (модуля) 3

2. Место дисциплины в структуре ОПОП 3

3. Требования к результатам освоения дисциплины (модуля) 4

4. Объем дисциплины (модуля) и виды учебной работы 5

5. Содержание дисциплины (модуля) 5

5.1. Содержание разделов и тем дисциплины (модуля). Все разделы и темы нумеруются 5

5.2. Разделы дисциплины и междисциплинарные связи с обеспечиваемыми (последующими) дисциплинами 7

5.3. Разделы и темы дисциплин (модулей) и виды занятий 8

6. Перечень семинарских, практических занятий и лабораторных работ 8

6.1. План самостоятельной работы студентов 9

6.2. Методические указания по организации самостоятельной работы студентов 10

7. Примерная тематика курсовых работ (проектов) 11

8. Учебно-методическое и информационное обеспечение дисциплины (модуля): .. 11

9. Материально-техническое обеспечение дисциплины (модуля) 11

10. Образовательные технологии 11

11. Оценочные средства (ОС): 12

11.1. Оценочные средства для входного контроля 12

11.2. Оценочные средства текущего контроля 12

11.3. Оценочные средства текущего контроля в форме тестирования 12

11.4. Оценочные средства для промежуточной аттестации 18

1. Цели и задачи дисциплины (модуля)

Учебная дисциплина «Техническая защита информации» обеспечивает приобретение знаний и умений в соответствии с государственным образовательным стандартом, содействует фундаментализации образования, формирование знаний в области технической защиты информации и навыков применения средств технической защиты информации в профессиональной деятельности.

Цели освоения учебной дисциплины «Техническая защита информации»:

1) развитие у студентов социально-личностных качеств: коммуникативности, организованности, ответственности, трудолюбия, целеустремленности;

2) формирование профессиональных знаний, навыков и умений в области технической защиты информации;

3) формирование практических навыков при работе со средствами технической защиты информации.

Задачи освоения учебной дисциплины**:**

1) формирование профессиональных знаний, навыков и умений по установке, настройке, эксплуатации и поддержании в работоспособном состоянии технических средств защиты информации с учетом установленных требований; изучение научно-технической информации, отечественного и зарубежного опыта по тематике исследования;

2) участие в проведении аттестации объектов, помещений, технических средств, систем, программ алгоритмов на предмет соответствия требованиям защиты информации;

3) получение навыков сбора и анализа исходных данных для проектирования систем защиты информации, определение требований, сравнительный анализ подсистем по показателям информационной безопасности;

4) совершенствование системы управления информационной безопасностью.

2. Место дисциплины в структуре ОПОП

Дисциплина «Техническая защита информации» является базовой дисциплиной профессионального цикла. Дисциплина является вводной в проблематику технической защиты информации. Взаимосвязь данной дисциплины через компетенции отражена в рабочем учебном плане и матрице компетенций. Дисциплина опирается на знания, полученные в ходе изучения дисциплин «Математический анализ», «Информатика», «Аппаратные средства вычислительной техники», «Электричество, магнетизм и волновая оптика», «Электротехника» которая должна быть освоена полностью и студенты должны владеть навыками применения методов технической защиты информации.

Дисциплина является предшествующей для таких дисциплин профессионального цикла как «Основы управления информационной безопасностью», «Техническая защита объектов критической информационной инфраструктуры», «Аттестация объектов информатизации», а так же для учебной и производственной практики и итоговой государственной аттестации. Изучение данной дисциплины позволяет приобрести первичные навыки, необходимые для изучения принципов обеспечения безопасности автоматизированных систем.

3. Требования к результатам освоения дисциплины (модуля)

Процесс изучения дисциплины (модуля) направлен на формирование следующей компетенции:

ОПК-7. Способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты.

В результате изучения дисциплины студент должен:

Знать:

- основные программно-аппаратные и технические средства защиты информации, применяемые на объектах информатизации;;

- основные характеристики программно-аппаратных и технических средств защиты информации, применяемых на объектах информатизации;

- особенности и возможности применения программно-аппаратных и технических средств защиты информации, применяемых на объектах информатизации для выявления и нейтрализации технических каналов утечки информации (ТКУИ).

Уметь:

- подготавливать к работе технические средства защиты информации, применяемые на объектах информатизации;;

- проводить установку, настройку технических средств защиты информации, применяемых на объектах информатизации;

- определять неисправности технических средств защиты информации, применяемых на объектах информатизации в соответствии с инструкцией по эксплуатации данных средств;

Владеть:

- навыками настройки технических средств защиты информации, применяемых на объектах информатизации;.

- навыками проведения контроля работоспособности и неисправности технических

средств защиты информации, применяемых на объектах информатизации в соответствии с инструкцией по эксплуатации данных средств.

4. Объем дисциплины (модуля) и виды учебной работы

Вид учебной работы	Всего часов / зачетных единиц	Семестры			
		7			
Аудиторные занятия (всего)	54/1,44	54/1,44			
В том числе:	-	-	-	-	-
Лекции	26/0,72	26/0,72			
Практические занятия (ПЗ)	26/0,72	26/0,72			
Семинары (С)					
Лабораторные работы (ЛР)					
КСР	2/0,06	2/0,06			
Контроль					
Самостоятельная работа (всего)	18/0,5	18/0,5			
В том числе:	-	-	-	-	-
Курсовой проект (работа)					
Расчетно-графические работы					
Реферат (при наличии)					
Другие виды самостоятельной работы					
Вид промежуточной аттестации (*зачет, экзамен*)	зачет	зачет			
Контактная работа (всего)	54/1,5	54/1,5			
Общая трудоемкость часы	72	72			
зачетные единицы	2	2			

5. Содержание дисциплины (модуля)

5.1. Содержание разделов и тем дисциплины (модуля). Все разделы и темы нумеруются

РАЗДЕЛ 1 Объекты информационной защиты.

Тема 1.1. Введение. Объекты информационной защиты.

Основные понятия**.** Классификация угроз безопасности информации. Информационные системы и необходимость их защиты.

Тема 1.2. Источники и носители конфиденциальной информации.

Источники конфиденциальной информации в информационных системах. Источники

конфиденциальной информации в информационных системах. Понятие утечки конфиденциальной информации.

Тема 1.3. Демаскирующие признаки объектов защиты и сигналов.

Демаскирующие признаки объектов наблюдения. Демаскирующие признаки сигналов.

РАЗДЕЛ 2 Технические каналы утечки информации.

Тема 2.1. Структура, классификация и основные характеристики технических каналов утечки информации.

Основные элементы канала реализации угроз безопасности информации. Классификация ТКУИ. ТКУИ, обрабатываемой техническими средствами. Схема ТКУИ.

Тема 2.2. Побочные электромагнитные излучения и наводки, электромагнитные излучения средств вычислительной техники.

Основные понятия и законы электромагнитных полей (ЭМП). Электромагнитные излучения систем средств вычислительной техники. Информативность побочных электромагнитных излучений и наводок (ПЭМИН). Паразитные связи и наводки.

Тема 2.3. Технические каналы утечки речевой и видовой информации.

Технические каналы утечки акустической (речевой) информации. Виброакустические технические каналы утечки речевой информации. Технические каналы утечки видовой информации. ТКУИ при ее передаче по каналам связи.

РАЗДЕЛ 3. Способы и средства добывания информации техническими средствами.

Тема 3.1. Технические средства доступа, перехвата и съема информации.

Способы перехвата речевой информации. Классификация закладных устройств. Устройства съема информации с телефонной линии.

Тема 3.2. Средства съема речевой информации.

Направленные микрофоны. Портативные диктофоны. Электронные стетоскопы.

Тема 3.3. Средства фотосъемки и видеонаблюдения.

Портативные средства фотосъемки. Портативные средства видеонаблюдения. Технические характеристики средств фотосъемки и видеонаблюдения.

РАЗДЕЛ 4. Методы, способы и средства технической защиты информации

Тема 4.1. Способы и средства защиты речевой информации от утечки по каналам связи и скрытие объектов наблюдения.

Методы и способы защиты персональных данных от утечки по техническим каналам. Пассивные и активные методы и способы защиты каналов утечки информации. Состав пассивных и активных средств защиты технических каналов утечки информации. Генераторы акустического шума.

Тема 4.2. Способы и средства предотвращения утечки информации через побочные электромагнитные излучения и наводки.

Методы и способы защиты информации, обрабатываемой в технических средствах передачи информации. Методы борьбы с утечками через ПЭМИН. Генераторы линейно-пространственного зашумления. Экранирование и компенсация информативных полей. Заземление технических средств.

Тема 4.3. Многофункциональные комплекты и комплексы для выявления каналов утечки информации.

Обнаружение и локализация закладных устройств, подавление их сигналов. Портативный комплект для обнаружения средств съема информации и выявления каналов ее утечки. Комплексы измерения ПЭМИН. Комплексы для измерения характеристик акустических сигналов

5.2. Разделы дисциплины и междисциплинарные связи с обеспечиваемыми (последующими) дисциплинами

№ п/п	Наименование обеспечиваемых (последующих) дисциплин	№№ разделов (тем) данной дисциплины, необходимых для изучения обеспечиваемых (последующих) дисциплин
1	Основы управления информационной безопасностью	4 (4.1-4.3)
2	Техническая защита объектов критической информационной инфраструктуры	1 (1.1-1.3)
3	Аттестация объектов информатизации	2 (2.1-2.3) 3 (3.1-3.3)
4	Практика по получению первичных профессиональных умений и навыков	1 (1.1-1.3) 2 (2.1-2.3) 3 (3.1-3.3) 4 (4.1-4.3)
5	Эксплуатационная практика	1 (1.1-1.3) 2 (2.1-2.3) 3 (3.1-3.3) 4 (4.1-4.3)

6	Проектно-технологическая практика	1 (1.1-1.3) 2 (2.1-2.3) 3 (3.1-3.3) 4 (4.1-4.3)

5.3. Разделы и темы дисциплин (модулей) и виды занятий

№ п/п	Наименование раздела	Наименование темы	Виды занятий в часах					
			Лекц.	Практ. зан.	Семин	Лаб. зан.	СРС	Всего
1.	***Раздел 1***	Тема 1.1	2	2			1	5
2.	***Раздел 1***	Тема 1.2	2	2			1	5
3.	***Раздел 1***	Тема 1.3	2	2			2	6
4.	***Раздел 2***	Тема 2.1	2	2			1	5
5.	***Раздел 2***	Тема 2.2	2	2			1	5
6.	***Раздел 2***	Тема 2.3	2	2			2	6
7.	***Раздел 3***	Тема 3.1	2	2			1	5
8.	***Раздел 3***	Тема 3.2	2	2			2	6
9.	***Раздел 3***	Тема 3.3	2	2			2	6
10.	***Раздел 4***	Тема 4.1	2	2			1	5
11.	***Раздел 4***	Тема 4.2	4	2			2	8
12.	***Раздел 4***	Тема 4.3	2	4			2	8

6. Перечень семинарских, практических занятий и лабораторных работ

№ п/п	№ раздела и темы дисциплины (модуля)	Наименование семинаров, практических и лабораторных работ	Трудоемкость (час.)	Оценочные средства	Формируемые компетенции
1	**2**	**3**	**4**	**5**	**6**
1.	***Раздел 1. Тема 1.1.***	ПЗ.1. Объекты защиты информации	2	Тестовый контроль по теме	ОПК-7
2.	***Раздел 1. Тема 1.2.***	ПЗ.2. Источники и носители конфиденциальной информации.	2	Тестовый контроль по теме	ОПК-7
3.	***Раздел 1. Тема 1.3.***	ПЗ. 3. Демаскирующие признаки сигналов.	2	Тестовый контроль по теме	ОПК-7
4.	***Раздел 2. Тема 2.1.***	ПЗ. 4. Характеристики технических каналов утечки информации.	2	Тестовый контроль по теме	ОПК-7
5.	***Раздел 2. Тема 2.2.***	ПЗ. 5. Побочные электромагнитные излучения и наводки средств вычислительной техники.	2	Тестовый контроль по теме	ОПК-7
6.	***Раздел 2. Тема 2.3.***	ПЗ. 6. Характеристики технических каналов утечки речевой и видовой информации.	2	Тестовый контроль по теме	ОПК7
7.	***Раздел 3. Тема 3.1.***	ПЗ. 7. Возможности и характеристики технических	2	Тестовый контроль	ОПК-7

		средств съема информации.		по теме	
8.	***Раздел 3. Тема 3.2.***	ПЗ. 8. Средства съема речевой информации.	2	Тестовый контроль по теме	ОПК-7
9.	***Раздел 3. Тема 3.3.***	ПЗ. 9. Средства съема видовой информации.	2	Тестовый контроль по теме	ОПК-7
10.	***Раздел 4. Тема 4.1.***	ПЗ 10. Технические средства защиты речевой информации от утечки по каналам связи	4	Тестовый контроль по теме	ОПК-7
11.	***Раздел 4. Тема 4.2.***	ПЗ. 11. Технические средства предотвращения утечки информации через побочные электромагнитные излучения и наводки	2	Тестовый контроль по теме	ОПК-7
12.	***Раздел 4. Тема 4.3.***	ПЗ. 12. Комплексы для выявления технических каналов утечки информации	4	Тестовый контроль по теме	ОПК-7

6.1. План самостоятельной работы студентов

№ нед.	Тема	Вид самостоятельной работы	Задание	Рекомендуемая литература	Количество часов
1-5	**1.1-1.3**	Решение задач к практическим занятиям Подготовка к защите лабораторных работ	Повторение и углубленное изучение учебного материала лекции, ПЗ с использованием конспекта лекций, литературы, Интернет - ресурсов	Учебный сайт	6
6-10	**2.1-2.3**	Решение задач к практическим занятиям Подготовка к защите лабораторных работ	Повторение и углубленное изучение учебного материала лекции, ПЗ с использованием конспекта лекций, литературы, Интернет - ресурсов	Учебный сайт	6
11-15	**3.1-3.3**	Подготовка к защите лабораторных работ	Повторение и углубленное изучение учебного материала	Учебный сайт	6

			лекции, ПЗ с использованием конспекта лекций, литературы, Интернет - ресурсов		
16-20	**4.1-4.3**	Решение задач к практическим занятиям Подготовка к защите лабораторных работ	Повторение и углубленное изучение учебного материала лекции, ПЗ с использованием конспекта лекций, литературы, Интернет - ресурсов	Учебный сайт	8
21		Подготовка доклада с презентацией		Учебный сайт	
22		Подведение итогов		Учебный сайт	

6.2. Методические указания по организации самостоятельной работы студентов

Текущая самостоятельная работа по дисциплине «Техническая защита информации», направленная на углубление и закрепление знаний студента, на развитие практических умений, включает в себя следующие виды работ:

- работа с лекционным материалом;
- подготовка к практическим занятиям;
- выполнение индивидуальных проектов;
- подготовка к лабораторным работам;
- подготовка к зачету.

Творческая проблемно-ориентированная самостоятельная работа по дисциплине «Техническая защита информации», направленная на развитие интеллектуальных умений, общекультурных и профессиональных компетенций, развитие творческого мышления у студентов, включает в себя следующие виды работ по основным проблемам курса:

- поиск, анализ, структурирование информации;
- выполнение графических работ, обработка и анализ данных;
- участие в конференциях, олимпиадах и конкурсах.

Оценка результатов самостоятельной работы организуется как единство двух форм: самоконтроль и контроль со стороны преподавателя.

Самоконтроль зависит от определенных качеств личности, ответственности за результаты своего обучения, заинтересованности в положительной оценке своего труда, материальных и моральных стимулов, от того насколько обучаемый мотивирован в достижении наилучших результатов. Задача преподавателя состоит в том, чтобы создать условия для выполнения самостоятельной работы (учебно-методическое обеспечение), правильно использовать различные стимулы для реализации этой работы (рейтинговая система), повышать её значимость, и грамотно осуществлять контроль самостоятельной деятельности студента (фонд оценочных средств).

7. Примерная тематика курсовых работ (проектов)

Курсовые работы (проекты) учебным планом не предусмотрены.

8. Учебно-методическое и информационное обеспечение дисциплины (модуля):

1. Фрязинов, А. В. Практикум по дисциплине "Защита персональных данных, автоматизация управленческой деятельности". Раздел 1 [Текст] : учеб.-практ. пособие / А. В. Фрязинов ; Иркут. гос. ун-т, Фак. сервиса и рекламы, Каф. прикл. информатики и документоведения. - Иркутск : Изд-во ИГУ, 2018. - 65 с.

2. Техническая защита информации: учебное пособие / Раков А. С., Маслов О. Н., Губарева О. Ю., Почепцов А. О., Гуреев В. О. Поволжский государственный университет телекоммуникаций и информатики, 2020. – 96с. https://e.lanbook.com/book/255575.

3. Глухарев М.Л., Исаева М.Ф. Технические средства защиты информации: Учебное пособие. Петербургский государственный университет путей сообщения Императора Александра I, 2018. – 55 с. https://e.lanbook.com/book/111736.

9. Материально-техническое обеспечение дисциплины (модуля)

Компьютерная лаборатория 323б (14 серверов) и лекционная аудитория 225, оснащенные мультимедийными средствами, электронной базой знаний, системой тестирования, выходом в глобальную сеть Интернет. Технические характеристики серверов обеспечивают возможность моделирования необходимого аппаратного обеспечения для работы с современными компьютерными системами хранения и обработки информации.

10. Образовательные технологии

Для достижения планируемых результатов обучения, в дисциплине «Криптографические методы защиты информации» используются различные образовательные технологии:

Информационно-развивающие технологии, направленные на формирование системы знаний, запоминание и свободное оперирование ими.

Используется лекционно-семинарский метод, самостоятельное изучение литературы, применение новых информационных технологий для самостоятельного пополнения знаний, включая использование технических и электронных средств информации.

Деятельностные практико-ориентированные технологии, направленные на формирование системы профессиональных практических умений при проведении экспериментальных исследований, обеспечивающих возможность качественно выполнять профессиональную деятельность.

Используется анализ, сравнение методов проведения химических исследований, выбор метода, в зависимости от объекта исследования в конкретной производственной ситуации и его практическая реализация.

Развивающие проблемно-ориентированные технологии, направленные на формирование и развитие проблемного мышления, мыслительной активности, способности видеть и формулировать проблемы, выбирать способы и средства для их решения. Используются виды проблемного обучения: освещение основных проблем общей и неорганической химии на лекциях, учебные дискуссии, коллективная деятельность в группах при выполнении лабораторных работ, решение задач повышенной сложности. При этом используются первые три уровня (из четырех) сложности и самостоятельности: проблемное изложение учебного материала преподавателем; создание преподавателем проблемных ситуаций, а обучаемые вместе с ним включаются в их разрешение; преподаватель создает проблемную ситуацию, а разрешают её обучаемые в ходе самостоятельной деятельности.

Личностно-ориентированные технологии обучения, обеспечивающие в ходе учебного процесса учет различных способностей обучаемых, создание необходимых условий для развития их индивидуальных способностей, развитие активности личности в учебном процессе. Личностно-ориентированные технологии обучения реализуются в результате индивидуального общения преподавателя и студента при защите лабораторных работ, при выполнении домашних индивидуальных заданий, решении задач повышенной сложности, на еженедельных консультациях.

11. Оценочные средства (ОС):

11.1. Оценочные средства для входного контроля

Не предусмотрено

11.2. Оценочные средства текущего контроля

Вопросы к практическим занятиям (12 тем). Представляют собой перечень вопросов,

проверяющих знание теоретического лекционного материала и тем, вынесенных на самостоятельную проработку:

Пз. 1 1. Демаскирующие признаки объектов защиты.
2. Классификация демаскирующих признаков.

Пз. 2 Конфиденциальная информация и её носители.

Пз. 3 1. Демаскирующие признаки аналоговых сигналов.
2. Демаскирующие признаки цифровых сигналов.

Пз. 4 1. Состав и характеристики технических каналов утечки информации.
2. Какие демаскирующие признаки сигналов позволяют выявить наличие закладного устройства в помещении?

Пз. 5 1. Что представляют собой ПЭМИН?
2. Характеристики аппаратуры перехвата и регистрации ПЭМИН.

Пз.6 1. Технические средства выявления демаскирующих признаков.
2. Методика и порядок проведения исследований по выявлению демаскирующих признаков.

Пз.7 1. Каким образом организуется процесс перехвата и восстановление информации ПЭМИН?
2. Какие характеристики СВТ используются при настройке аппаратуры перехвата ПЭМИН?

Пз. 8 1. Каким образом организуется процесс перехвата и восстановление речевой информации?
2. В чем заключается принцип формирования акустического канала утечки информации?

Пз. 9 Каким образом организуется процесс перехвата и восстановление видовой информации?

Пз. 10 1. Аппаратура акустической защиты речевой информации. Проблемы применения.
2. Принципы построения генераторов акустического и вибрационного шумов.

Пз. 11 1. Активные и пассивные средства защиты от ПЭМИН.
2. Подавление ПЭМИН с помощью генераторов линейно-пространственного зашумления.

Пз. 12 1. Принципы построения и функционирования программно-аппаратных комплексов.
2. Основные технические характеристики программно-аппаратных комплексов.
3. Порядок проведения исследований с помощью многофункциональных комплексов.

11.3. Оценочные средства для текущего контроля в форме тестирования

Тестовые вопросы для проверки сформированности компетенции

ОПК-7. Способность определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты.

1. К средствам защиты от ПЭМИ относятся?
А) Генераторы линейно-пространственного зашумления;
Б) Генераторы НЧ;

В) Генераторы белого шума
Г) Генераторы «цветного» шума.

2. К средствам АВАК защиты относятся (выберите все возможные варианты)?
А) Генераторы АВАК сигналов;
Б) Виброизлучатели;
В) Пьезоизлучатели;
Г) «Глушилки».

3. Параметры антенных устройств (выберите все возможные варианты)?:
А) диаграмма направленности;
Б) коэффициент усиления;
В) сопротивление;
Г) напряжение.

4. Какой физический эффекты используют в электронных стетоскопах?:
А) твердотельный;
Б) воздушный;
В) пьезо-электрический;
Г) магнито-стрикционный.

5. ПЭМИ можно регистрировать с помощью? (выберите все возможные варианты):
А) спектрографа;
Б) спектроанализатора;
В) осцилографа;
Г) минивольтметра;
Д) селективного мультивольтметра

6. К пассивным методам защиты от ПЭМИ относится (выберите неправильный ответ)?:
А) Экранирование;
Б) Заземление;
В) Заводнение;
Г) Генерирование шума.

7. Фильтры бывают (выберите все возможные варианты)?
А) Активными;
Б) Пассивными;
В) Полупассивными;
Г) Неактивными

8. Средство защиты от ПЭМИ имеет название?
А) «Гренада»;
Б) «Блокада»;
В) «Турбо»;
Г) «Баррикада»

9. В состав «RS-turbo» входит?:
А) Анализатор спектра;
Б) Сканирующий приемник;
В) Детектор слабого сигнала;
Г) Селективный микровольтметр.

10. «RS-turbo» в автоматизированном режиме определяет? (выберите все возможные варианты):

А) Опасные частоты;

Б) Подозрительные частоты;

В) Принципиально-опасные частоты;

Г) Спектральный частоты.

11. В состав лабораторной установки по измерению ПЭМИ в ходят (выберите все возможные варианты)?:

А) осциллограф;

Б) вольтметр;

В) ПЭВМ;

Г) антенная система;

Д) ПО «Зебра»

12. Название нелинейного локатора, используемого на ЛР?:

А) «Топаз»;

Б) «Бумеранг»;

В) «Катран»;

Г) «Капкан».

13. Центральная частота 2 октавы (при оценке защищенности)?:

А) 125;

Б) 500;

В) 1000;

Г) 2000

14. Какая из зон характеризует наводки информативного сигнала на ВТСС?:

А) 1;

Б) 2;

В) 3;

Г) 5.

15. СЗИ должно иметь?:

А) Формуляр;

Б) Описание;

В) Положение;

Г) Сертификат.

16. Расшифруйте аббревиатуру «СЗЗ»:

А) Специальный защитный знак;

Б) Средство защиты зоны;

В) Система защитных заграждений.

Г) Средства защиты зданий.

17. Сведения о проведенных специсследованиях заносятся в?:

А) Спецблокнот;

Б) Протокол;

В) Рабочую тетрадь;

Г) Таблицу.

18. Для расчета ПЭМИ от ЭЛТ требуется?:
А) Разрешение экрана, частота излучения;
Б) Разрешение экрана, частота генератора;
В) Разрешение экрана, частота кадров;
Г) Частота развертки, разрешающая способность.

19. Установите порядок действий при работе с многофункциональным комплексом «RS-turbo»:
А) локализация закладного устройства;
Б) сканирование;
В) обнаружение;
Г) классификация.

20. К ДП аналоговых сигналов относятся (выберите все возможные варианты)?
А) Вид модуляции;
Б) Частота;
В) Скважность;
Г) Амплитуда.

21. К ДП дискретных сигналов относятся (выберите все возможные варианты)?
А) Вид модуляции;
Б) Частота следования импульсов;
В) Скважность;
Г) Время.

22. По информативности излучения СВТ делятся?
А) Принципиально неинформативные;
Б) Потенциально неинформативные;
В) Принципиально информативные.
Г) Условно информативные

23. К основным элементам канала реализации угроз безопасности информации относятся (выберите все возможные варианты):
А) Физическое поле;
Б) Объект разведки;
В) Локальная среда;
Г) Радиоэфир.

24. Физический принцип действия направленных микрофонов:
А) Переключение звуковых колебаний;
Б) Умножение составляющих звуковых колебаний;
В) Сложение в фазе звуковых колебаний;
Г) Фильтрация сигналов.

25. В каком диапазоне частот сосредоточено 95% энергии речевого сигнала?:
А) 25-250 Гц;
Б) 500-2500;
В) 175-5600 Гц;
Г) 20-20000 Гц
26. Единица измерения виброускорения?:
А) Гц;
Б) м/с*с;

В) дБ;
Г) Па.

27. Физические основы возникновения ТКУИ в ВТСС (выберите все возможные варианты)?:
А) Обратный эффект Фарадея;
Б) Эффект Виллари;
В) Пьезоэффект;
Г) Эффект Галилео;
Д) Прямой эффект Ньютона

28. Качество принимаемой информации при использовании лазерного микрофона зависит от следующих факторов?:
А) параметров геомагнитной обстановки;
Б) параметров атмосферы;
В) уровня фоновых акустических шумов;
Г) параметров используемого лазера;
Д) артериального давления

29. Сила света измеряется в :
А) Ньютонах;
Б) Канделах;
В) Паскалях;
Г) Стеррадианах

30. Основные элементы лазера (выберите все возможные варианты)?:
А) Медиатор;
Б) Компаратор;
В) Резонатор;
Г) Устройство накачки.

31. Для измерения ПЭМИ могут использоваться? (выберите все возможные варианты):
А) Спектроанализаторы;
Б) Селективные микровольтметры;
В) Мультивольтметры;
Г) Вариометры.

32. Нелинейный локатор фиксирует излучения от:
А)t-c-p перехода;
Б) p-n-p перехода;
В)r-n-b перехода;
Г) b-t-b перехода.

33. Сколько октав используется для определения показателей защищенности объекта?:
А) 12;
Б) 4;
В) 8;
Г) 5;
Д) 7.

34. Сколько зон используется для определения показателей защищенности объекта по каналу ПЭМИН?:

А) 1;
Б) 2;
В) 3;
Г) 4;
Д) 5.

35. В состав лабораторной установки по выявлению ПЭМИ входит:

А) генератор, осциллограф, комплект кабелей;
Б) генератор, спектроанализатор, комплект кабелей;
В) антенна, селективный микровольтметр, комплект кабелей;
Г) антенна, осциллограф, комплект кабелей

11.4. Оценочные средства для промежуточной аттестации

(в форме зачета).

Проверяется степень усвоения теоретических и практических знаний, приобретенных умений на репродуктивном и продуктивном уровне.

Примерный перечень вопросов и заданий к зачету

Раздел 1 «Объекты информационной защиты»

1.1 Источники конфиденциальной информации в информационных системах.
1.2 Источники и носители информации в средствах вычислительной техники.
1.3 Сущность энтропийного подхода к оценке количества информации.
1.4 Количество информации по Шеннону.
1.5 Демаскирующие признаки (ДП). Технические демаскирующие признаки объекта. Основные понятия.
1.6 Классификация демаскирующих признаков.
1.7 Технические ДП.
1.8 Демаскирующие признаки объектов наблюдения.
1.9 Особенности видовых признаков в оптическом и радиодиапазонах. ДП объектов в ИК - диапазоне.
1.10 ДП объектов радиолокационного наблюдения.
1.11 Демаскирующие признаки аналоговых сигналов.
1.12 Демаскирующие признаки цифровых сигналов.

Раздел 2 «Технические каналы утечки информации»

2.1 Побочные электромагнитные излучения и наводки (ПЭМИН). Общие положения
2.2 Электромагнитные излучения систем СВТ
2.3 Классификация ТКУ И
2.4 ТКУ речевой информации
2.5 Краткие сведения по акустике
2.6 Звуковое давление
2.7 Акустические и электрические уровни
2.8 Акустические каналы
2.9 Направленные микрофоны
2.10 Проводные системы, портативные диктофоны и электронные стетоскопы
2.11 Виброакустические технические каналы утечки речевой информации
2.12 Акустоэлектрические каналы утечки речевой информации
2.13 Оптико-электронный технический канал утечки речевой информации
2.14 Параметрические технические каналы утечки речевой информации
2.15 ТКУ видовой информации

2.16 Каналы утечки информации при ее передаче по каналам связи

Раздел 3. «Способы и средства добывания информации техническими средствами»

3.1 Классификация технической разведки

3.2 Возможности видов технической разведки

3.3 Характеристики аппаратуры перехвата речевой информации

3.4 Характеристики аппаратуры перехвата видовой информации

3.5 Характеристики аппаратуры перехвата ПЭМИН

3.6 Классификация устройств съема информации с телефонной линии

3.7 Метод ВЧ навязывания (прослушивание помещений через микрофон телефонного аппарата)

3.8 Использование выносных микрофонов

3.9 Перехват сигналов сотовых телефонов.

3.4 Перечень теоретических вопросов к зачету

Раздел 4 «Методы, способы и средства технической защиты информации»

4.1 Скрытие речевой информации в каналах связи

4.2 Энергетическое скрытие акустических информативных сигналов

4.3 Скрытие речевой информации в каналах связи.

4.4 Способы и средства обнаружения закладных устройств

4.5 Классификация средств обнаружения и локализации закладных устройств

4.6 Средства обнаружения излучений закладных устройств

4.7 Сканирующие радиоприемники

4.8 Средства обнаружения неизлучающих закладок

4.9 Принцип действия нелинейного локатора.

4.10 Нелинейный локатор «Катран». Назначение, состав, основные характеристики, режимы работы.

4.11 Многофункциональные комплекты для выявления каналов утечки информации

4.12 Портативный комплект для обнаружения средств съема информации и выявления каналов ее утечки «ПКУ-6М»

4.13 Портативный комплект для обнаружения средств съема информации и выявления каналов ее утечки «Пиранья»

4.14 Комплекс RS turbo

4.15. Радиотехнические системы передачи информации.

4.16. Радиолокационная система охраны периметра и территории объектов.

4.17. Классификация помех.

4.18. Естественные аддитивные помехи.

4.19. Искусственные аддитивные помехи.

4.20. Мультипликативные помехи.

4.21. Особенности частотных диапазонов.

4.22. Распространение радиоволн.

4.23. Диапазоны волн (частот).

4.24 Подавление опасных сигналов акустоэлектрических преобразователей телефонных линиях

4.25 Пассивные методы защиты от утечки информации по акустоэлектрическому каналу

4.26 Активные методы защиты от утечки информации по акустоэлектрическому каналу

4.27 Экранирование как пассивный способ защиты от утечек по техническим каналам

4.28 Заземление технических средств и подавление информационных сигналов в цепях заземления.

Разработчики:

_____	___профессор_____	_Ерохин В.В._____
(подпись)	(занимаемая должность)	(Ф.И.О.)

Программа составлена в соответствии с требованиями ФГОС ВО и учитывает рекомендации ПООП по направлению и профилю подготовки **10.03.01 Информационная безопасность**.

Программа рассмотрена на заседании кафедры радиофизики и радиоэлектроники
«20» 03 2020 г. Протокол № 8

И.о.зав. кафедрой  Колесник С.Н.