МИНОБРНАУКИ РОССИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО «ВГУ»)

УТВЕРЖДАЮ

Заведующий кафедрой
технологий обработки и защиты информации

_____ / Сирота А.А.

23.04.2024 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Б1.О.51 Защита информации от утечки по техническим каналам

1. Код и наименование направления подготовки/специальности:

10.05.01 Компьютерная безопасность

2. Специализация:

Безопасность компьютерных систем и сетей

Математические методы защиты информации

3. Квалификация выпускника: специалист

4. Форма обучения: очная

5. Кафедра, отвечающая за реализацию дисциплины:
технологий обработки и защиты информации

6. Составители программы:

Головинский Павел Абрамович, профессор

7. Рекомендована: НМС ФКН (протокол № 5 от 05.03.2024)

8. Учебный год: 2026-2027 **Семестр:** 6

9. **Цели и задачи учебной дисциплины**

Целью дисциплины является изучение современных методов и систем защиты информации от утечки по техническим каналам для обеспечения компетенций по комплексной защите функционирования информационных объектов различной степени секретности с использованием автоматизированных систем контроля, а также системных методов пассивной и активной защиты.

Основные задачи дисциплины:

1. Рассмотреть угрозы утечки и воздействия на информацию через технические каналы.

2. Ознакомиться с физическими процессами, лежащими в основе технических каналов утечки информации.

3. Рассмотреть основные методы и средства технической защиты информации.

4. Изучить приборные средства контроля технических каналов утечки информации.

5. Разобрать комплексную методологию защиты от угроз информации по техническим каналам с учетом системного анализа и аттестацию объектов защиты.

10. Место учебной дисциплины в структуре ООП:

дисциплина относится к обязательной части учебного плана.

11. Планируемые результаты обучения по дисциплине/модулю (знания, умения, навыки), соотнесенные с планируемыми результатами освоения образовательной программы (компетенциями) и индикаторами их достижения:

Код	Название компетенции	Код(ы)	Индикатор(ы)	Планируемые результаты обучения
ОПК-5	Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации.	ОПК-5.14	Знает способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации	Знает способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации
		ОПК-5.15	Знает организацию защиты информации от утечки по техническим каналам на объектах информатизации	Знает организацию защиты информации от утечки по техническим каналам на объектах информатизации
		ОПК-5.16	Знает возможности технических средств перехвата информации	Знает возможности технических средств перехвата информации
		ОПК-5.17	Умеет анализировать и оценивать угрозы информационной безопасности объекта по техническим каналам	Умеет анализировать и оценивать угрозы информационной безопасности объекта по техническим каналам
		ОПК-5.18	Знает нормативные документами в области технической защиты информации	Знает нормативные документами в области технической защиты информации
		ОПК-5.19	Владеет методами и средствами технической защиты информации	Владеет методами и средствами технической защиты информации
ОПК-6	Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в компьютерных системах и	ОПК-6.1	Знает систему нормативных правовых актов и стандартов по лицензированию в области обеспечения защиты государственной тайны, технической защиты	Знает систему нормативных правовых актов и стандартов по лицензированию в области обеспечения защиты государственной тайны, технической защиты

	сетях в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю		конфиденциальной информации, по аттестации объектов информатизации и сертификации средств защиты информации	конфиденциальной информации, по аттестации объектов информатизации и сертификации средств защиты информации
		ОПК-6.2	Знает задачи органов защиты государственной тайны и служб защиты информации на предприятиях	Знает задачи органов защиты государственной тайны и служб защиты информации на предприятиях
		ОПК-6.3	Знает систему организационных мер, направленных на защиту информации ограниченного доступа	Знает систему организационных мер, направленных на защиту информации ограниченного доступа
		ОПК-6.4	Знает нормативные, руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации ограниченного доступа	Знает нормативные, руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации ограниченного доступа
		ОПК-6.5	Знает основные угрозы безопасности информации и модели нарушителя компьютерных систем	Знает основные угрозы безопасности информации и модели нарушителя компьютерных систем
		ОПК-6.6	Умеет разрабатывать модели угроз и модели нарушителя компьютерных систем	Умеет разрабатывать модели угроз и модели нарушителя компьютерных систем
		ОПК-6.7	Умеет разрабатывать проекты инструкций, регламентов, положений и приказов, регламентирующих защиту информации ограниченного доступа в организации	Умеет разрабатывать проекты инструкций, регламентов, положений и приказов, регламентирующих защиту информации ограниченного доступа в организации
		ОПК-6.8	Умеет определить политику контроля доступа работников к информации ограниченного доступа	Умеет определить политику контроля доступа работников к информации ограниченного доступа
		ОПК-6.9	Умеет формулировать основные требования, предъявляемые к физической защите объекта и пропускному режиму в организации	Умеет формулировать основные требования, предъявляемые к физической защите объекта и пропускному режиму в организации
		ОПК-6.10	Умеет применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценивания защищенности компьютерной системы	Умеет применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценивания защищенности компьютерной системы
ОПК-9	Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития методов защиты информации в операционных системах, компьютерных сетях и системах управления базами данных, а также методов и средств защиты информации от утечки по техническим каналам, сетей и систем передачи информации	ОПК-9.1	Знает технические каналы утечки информации	Знает технические каналы утечки информации
		ОПК-9.2	Знает возможности технических средств перехвата информации	Знает возможности технических средств перехвата информации
		ОПК-9.3	Умеет организовать защиту информации от утечки по техническим каналам на объектах информатизации	Умеет организовать защиту информации от утечки по техническим каналам на объектах информатизации
		ОПК-9.4	Умеет пользоваться нормативными документами в области технической защиты информации	Умеет пользоваться нормативными документами в области технической защиты информации
		ОПК-9.13	Знает способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации	Знает способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации

		ОПК-9.14	Знает основы физической защиты объектов информатизации	Знает основы физической защиты объектов информатизации
		ОПК-9.15	Умеет анализировать и оценивать угрозы информационной безопасности объекта	Умеет анализировать и оценивать угрозы информационной безопасности объекта
		ОПК-9.16	Владеет методами и средствами технической защиты информации	Владеет методами и средствами технической защиты информации
		ОПК-9.17	Владеет методами расчета и инструментального контроля показателей эффективности технической защиты информации	Владеет методами расчета и инструментального контроля показателей эффективности технической защиты информации

12. Объем дисциплины в зачетных единицах/час. — 4/144.

Форма промежуточной аттестации 6 семестр – экзамен.

13. Трудоемкость по видам учебной работы

Вид учебной работы		Трудоемкость	
		Всего	По семестрам
			6 семестр
Аудиторные занятия		72	72
в том числе:	лекции	36	36
	практические		
	лабораторные	36	36
Самостоятельная работа		36	36
Экзамен		36	36
Итого:		144	144

13.1. Содержание дисциплины

№ п/п	Наименование раздела дисциплины	Содержание раздела дисциплины	Реализация раздела дисциплины с помощью онлайн-курса, ЭУМК*
1. Лекции			
1.1	Технические каналы утечки информации	1. Классификация иностранной технической разведки. Возможности видов технической разведки. Основные этапы и процедуры добывания информации технической разведкой. Задачи систем защиты информации. Общие понятия. 2. Технические каналы утечки информации. Структура, классификация и основные характеристики. Технические каналы утечки информации, обрабатываемой ТСПИ (техническими средствами приёма, обработки и хранения информации).	Создан электронный онлайн-курс, размещены материалы к лекциям. Размещены индивидуальные задания для выполнения лабораторных работ.

1.2	Утечка информации по электромагнитным каналам	3. Основные уравнения электромагнитного поля. Элементарный электрический излучатель. Элементарный магнитный излучатель. Электромагнитные каналы утечки информации ТСПИ. Электрические каналы утечки информации. Наводки электромагнитных излучений ТСПИ. Параметрический канал утечки информации. Электрические линии связи. 4. Средства передачи электрических сигналов. Виды проводных электрических линий связи и их параметры. 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.	Создан электронный онлайн-курс, размещены материалы к лекциям. Размещены индивидуальные задания для выполнения лабораторных работ.
1.3	Технические каналы утечки речевой информации	5. 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. 6. Виброакустические технические каналы утечки речевой информации. Акустоэлектрические каналы утечки речевой информации. Оптико-электронный технический канал утечки речевой информации. Параметрические технические каналы утечки речевой информации. Звуковые сигналы. Маскировка звуковых сигналов. Понятность и разборчивость речи. Частотный диапазон и спектры. Звуковое поле в помещении. Звуковой фон в помещении. 7. 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.	Создан электронный онлайн-курс, размещены материалы к лекциям. Размещены индивидуальные задания для выполнения лабораторных работ.

1.4	Скрытие и защита информации от утечки по техническим каналам	8. Особенности задач охраны различных типов объектов. Общие принципы обеспечения безопасности объектов. Система охранно-тревожной сигнализации. Система контроля и управления доступом. Телевизионные системы. Система пожарной сигнализации. Периметровая охрана. 9. Концепция и методы инженерно-технической защиты информации. Экранирование электромагнитных волн. Электромагнитное экранирование и развязывающие цепи. Подавление емкостных паразитных связей. Подавление индуктивных паразитных связей. Экранирование проводов и катушек индуктивности. Экранированные помещения. Безопасность оптоволоконных кабельных систем. Заземление технических средств и подавление информационных сигналов в цепях заземления. Фильтрация информационных сигналов. 10. Основные сведения о помехоподавляющих фильтрах. Выбор типа фильтра. Пространственное и линейное зашумление. Способы предотвращения утечки информации через ПЭМИН ПК. Устройства контроля и защиты слаботочных линий и сети. Особенности слаботочных линий и сетей как каналов утечки информации. Рекомендуемые схемы подключения анализаторов к электросиловым и телефонным линиям в здании. Устройства контроля и защиты проводных линий от утечки информации. Скрытие и защита от утечки информации по акустическому и виброакустическому каналам. Скрытие речевой информации в телефонных системах с использованием криптографических методов. Понятие о квантовой криптографии.	Создан электронный онлайн-курс, размещены материалы к лекциям. Размещены индивидуальные задания для выполнения лабораторных работ.
1.5	Технические средства выявления каналов утечки информации	11. Общие сведения. Индикаторы электромагнитного поля. Сканирующие радиоприемники. Анализаторы спектра, радиочастотомеры. Многофункциональные комплекты для выявления каналов утечки информации. 12. Портативный комплект для обнаружения средств съема информации и выявления каналов ее утечки ПКУ-6М. Портативный комплект для обнаружения средств съема информации и выявления каналов ее утечки «Пиранья». Комплекс RS turbo. Комплексы измерения ПЭМИН. Нелинейные локаторы. Комплекс для измерения характеристик акустических сигналов «Спрут-7». 13. Металлодетекторы. Портативная рентгенотелевизионная установка «НОРКА». Досмотровые эндоскопы. Secret Net 5.0. Электронный замок «Соболь». USB-ключ. Считыватели Proximity. Технология защиты информации на основе смарт-карт. Кейс «Тень». Устройство для быстрого уничтожения информации на жестких магнитных дисках «Стек-Н».	Создан электронный онлайн-курс, размещены материалы к лекциям. Размещены индивидуальные задания для выполнения лабораторных работ.
1.6	Технический контроль и аттестация объектов информатизации по	14. Цели и задачи технического контроля эффективности мер защиты информации. Порядок проведения контроля защищенности	Создан электронный онлайн-курс, размещены материалы к

	требованиям безопасности информации	информации на объекте ВТ от утечки по каналу ПЭМИ. Методы испытаний ПЭВМ. Порядок проведения контроля защищенности АС от НСД. Методы контроля побочных электромагнитных излучений генераторов технических средств. Порядок проведения контроля защищенности выделенных помещений от утечки акустической речевой информации. Общие положения. Подготовительный этап контроля. Акустический и виброакустический контроль. 15. Методика контроля. Выбор контрольных точек иразмещение элементов измерительных комплексов. Калибровка передающего измерительного комплекса. Размещение акустического излучателя передающего измерительного комплекса. 16. Измерение отношений «сигнал/шум» в контрольных точках при инструментальном контроле рабочих помещений, не оборудованных системой звукоусиления. Измерение отношений «сигнал/шум» в контрольных точках при инструментальном контроле рабочих помещений, оборудованных системой звукоусиления. Контроль технических средств и систем на наличие акустоэлектрических преобразований. Подготовительный этап контроля. Методика контроля. 17. Мероприятия по выявлению и оценке свойств каналов утечки информации. Специальные проверки. Специальные обследования. Специальные исследования. Специальные исследования акустических и виброакустических каналов. Специальные исследования акустоэлектрических преобразований. Специальные исследования технических средств и систем на возможность утечки информации за счет побочных электромагнитных излучений и наводок.	лекциям. Размещены индивидуальные задания для выполнения лабораторных работ.
2. Лабораторные занятия			
2.1	Технические каналы утечки информации	1. Спектры сигналов	Создан электронный онлайн-курс, размещены материалы к лекциям. Размещены индивидуальные задания для выполнения лабораторных работ.
2.2	Утечка информации по электромагнитным каналам	2. Предварительное обследование объекта защиты с помощью мобильных приложений. 3. Изучения состава и порядка работы с комплексом СИГУРД–М19.	Создан электронный онлайн-курс, размещены материалы к лекциям. Размещены индивидуальные задания для выполнения лабораторных работ.
2.3	Технические каналы утечки речевой информации	4. Определение источников сигнала и утечек по электромагнитному каналу прибором «Пиранья». 5. Определение источников сигнала и утечек по акустическому и виброакустическому каналам прибором «Пиранья».	Создан электронный онлайн-курс, размещены материалы к лекциям. Размещены индивидуальные задания для выполнения

			лабораторных работ.
2.4	Скрытие и защита информации от утечки по техническим каналам	6. Пассивная защита от утечек информации по техническим каналам. 7. Определение источников и характеристик акустических сигналов комплексом «СМАРТ».	Создан электронный онлайн-курс, размещены материалы к лекциям. Размещены индивидуальные задания для выполнения лабораторных работ.
2.5	Технические средства выявления каналов утечки информации	8. Определение источников и характеристик электромагнитных сигналов комплексом КАССАНДРА. 9. Постановка акустических помех с помощью прибора ГШ-1.	Создан электронный онлайн-курс, размещены материалы к лекциям. Размещены индивидуальные задания для выполнения лабораторных работ.
2.6	Технический контроль и аттестация объектов информатизации по требованиям безопасности информации	10. Подготовка актов обследования объекта защиты по результатам технических испытаний	Создан электронный онлайн-курс, размещены материалы к лекциям. Размещены индивидуальные задания для выполнения лабораторных работ.

13.2. Темы (разделы) дисциплины и виды занятий

№ п/п	Наименование темы (раздела) дисциплины	Виды занятий (количество часов)				
		Лекции	Практические	Лабораторные	Самостоятельная работа	Всего
1	Технические каналы утечки информации	4		4	4	12
2	Утечка информации по электромагнитным каналам	6		6	6	18
3	Технические каналы утечки речевой информации	6		6	6	18
4	Скрытие и защита информации от утечки по техническим каналам	6		6	6	18
5	Технические средства выявления каналов утечки информации	6		6	6	18
6	Технический контроль и аттестация объектов информатизации по требованиям безопасности информации	8		8	8	24
	Итого:	36		36	36	108

14. Методические указания для обучающихся по освоению дисциплины:

Освоение дисциплины складывается из аудиторной работы (учебной деятельности, выполняемой под руководством преподавателя) и внеаудиторной работы (учебной деятельности, реализуемой обучающимся самостоятельно).

Аудиторная работа состоит из работы на лекциях и выполнения практических (или лабораторных) заданий в объёме, предусмотренном учебным планом. Лекция представляет собой последовательное и систематическое изложение учебного материала, направленное на знакомство обучающихся с основными понятиями и теоретическими положениями изучаемой дисциплины. Лекционные занятия формируют базу для практических (или лабораторных) занятий, на которых полученные теоретические знания применяются для решения конкретных практических задач. Обучающимся для успешного освоения дисциплины рекомендуется вести конспект лекций и практических (лабораторных) занятий.

Самостоятельная работа предполагает углублённое изучение отдельных разделов дисциплины с использованием литературы, рекомендованной преподавателем, а также конспектов лекций, презентационным материалом (при наличии) и конспектов практических (лабораторных) занятий. В качестве плана для самостоятельной работы может быть использован раздел 13.1 настоящей рабочей программы, в котором зафиксированы разделы дисциплины и их содержание. В разделе 13.2 рабочей программы определяется количество часов, отводимое на самостоятельную работу по каждому разделу дисциплины. Большее количество часов на самостоятельную работу отводится на наиболее трудные разделы дисциплины. Для самостоятельного изучения отдельных разделов дисциплины используется перечень литературы и других ресурсов, перечисленных в пунктах 15 и 16 настоящей рабочей программы.

Успешность освоения дисциплины определяется систематичностью и глубиной аудиторной и внеаудиторной работы обучающегося.

При использовании дистанционных образовательных технологий и электронного обучения выполнять все указания преподавателей, вовремя подключаться к online занятиям, ответственно подходить к заданиям для самостоятельной работы.

15. Перечень основной и дополнительной литературы, ресурсов интернет, необходимых для освоения дисциплины

а) основная литература:

№ п/п	Источник
1	Нестеров, С. А. Основы информационной безопасности / С. А. Нестеров. — 3-е изд., стер. — Санкт-Петербург : Лань, 2024. — 324 с. — ISBN 978-5-507-49077-6. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/370967
2	Киренберг, А. Г. Защита информации от утечки по техническим каналам : учебное пособие / А. Г. Киренберг, В. О. Коротин. — Кемерово : КузГТУ имени Т.Ф. Горбачева, 2023. — 222 с. — ISBN 978-5-00137-407-7. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/399665
3	Голиков, А. М. Защита информации от утечки по техническим каналам : учебное пособие / А. М. Голиков. — Москва : ТУСУР, 2015. — 256 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/110328

б) дополнительная литература:

№ п/п	Источник
1	Краковский, Ю. М. Методы и средства защиты информации : учебное пособие для вузов / Ю. М. Краковский. — Санкт-Петербург : Лань, 2024. — 272 с. — ISBN 978-5-507-48601-4. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/385979
2	Программно-аппаратные средства защиты информации : учебное пособие / С. А. Зырянов, М. А. Кувшинов, И. А. Огнев, И. В. Никрошкин. — Новосибирск : НГТУ, 2023. — 80 с. — ISBN 978-5-7782-4905-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/404549

3	Техническая защита информации: практикум : учебное пособие / Л. В. Аршинский, А. А. Бутин, Н. И. Глухов [и др.]. — Иркутск : ИрГУПС, 2022. — 76 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/342083

в) информационные электронно-образовательные ресурсы (официальные ресурсы интернет)*:

№ п/п	Ресурс
1	ЗНБ ВГУ: https://lib.vsu.ru/
2	Электронно-библиотечная система "Университетская библиотека online": http://biblioclub.ru/
3	Электронно-библиотечная система "Лань": https://e.lanbook.com/

16. Перечень учебно-методического обеспечения для самостоятельной работы

№ п/п	Источник
1	Голиков, А. М. Защита информации от утечки по техническим каналам : учебное пособие / А. М. Голиков. — Москва : ТУСУР, 2015. — 256 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/110328
2	Техническая защита информации: практикум : учебное пособие / Л. В. Аршинский, А. А. Бутин, Н. И. Глухов [и др.]. — Иркутск : ИрГУПС, 2022. — 76 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/342083

17. Образовательные технологии, используемые при реализации учебной дисциплины, включая дистанционные образовательные технологии (ДОТ, электронное обучение (ЭО), смешанное обучение):

При реализации дисциплины могут использоваться технологии электронного обучения и дистанционные образовательные технологии на базе портала edu.vsu.ru, а также другие доступные ресурсы сети Интернет.

18. Материально-техническое обеспечение дисциплины:

1. Учебная аудитория (394018, г. Воронеж, площадь Университетская, д. 1, ауд. 303П) для проведения лабораторных работ, укомплектованная специализированной мебелью и техническими средствами обучения, служащими для представления учебной информации большой аудитории: наборами демонстрационного оборудования и учебно-наглядных пособий, обеспечивающими тематические иллюстрации, соответствующие рабочей программе дисциплины, оснащенная компьютерной техникой.

2. Учебные аудитории для проведения групповых и индивидуальных консультаций, укомплектованные специализированной мебелью и техническими средствами обучения, оснащенные компьютерной техникой.

3. Помещение для самостоятельной работы студентов, оснащенное компьютерной техникой с возможностью подключения к сети Интернет и обеспечением доступа в электронную информационно-образовательную среду.

4. Лабораторное оборудование: Комплекс СИГУРД–М19, комплекс «СМАРТ», комплекс Кассандра СКМ-21, блок «Соната», прибор СМАРТ-ГШ-1, прибор «Пиранья».

19. Оценочные средства для проведения текущей и промежуточной аттестаций

Порядок оценки освоения обучающимися учебного материала определяется содержанием следующих разделов дисциплины:

№ п/п	Наименование раздела дисциплины (модуля)	Компетенции	Индикаторы достижения компетенции	Оценочные средства
1.	Разделы 1-6	ОПК-5 ОПК-6 ОПК-9	ОПК-5.14 ОПК-5.15 ОПК-5.16 ОПК-5.17 ОПК-5.18 ОПК-5.19 ОПК-6.1 ОПК-6.2 ОПК-6.3 ОПК-6.4 ОПК-6.5 ОПК-6.6 ОПК-6.7 ОПК-6.8 ОПК-6.9 ОПК-6.10 ОПК-9.1 ОПК-9.2 ОПК-9.3 ОПК-9.4 ОПК-9.13 ОПК-9.14 ОПК-9.15 ОПК-9.16 ОПК-9.17	Лабораторные работы. Тестовые задания.
Промежуточная аттестация форма контроля – экзамен				Вопросы к экзамену

20. Типовые оценочные средства и методические материалы, определяющие процедуры оценивания

20.1. Текущий контроль успеваемости

Текущий контроль успеваемости по дисциплине осуществляется с помощью следующих оценочных средств: устный опрос на лекционных занятиях; отчеты о выполнении лабораторных работ, ответы на тестовые вопросы.

Примерный перечень применяемых оценочных средств

Наименование оценочного средства	Представление оценочного средства в фонде	Критерии оценки
1. Устный опрос на лабораторных занятиях	Вопросы по темам/разделам дисциплины	Правильный ответ – зачтено, неправильный или принципиально неточный ответ – не зачтено

2. Тесты для проверки знаний	Теоретические вопросы по темам/разделам дисциплины	Шкала оценивания соответствует приведенной ниже
3. Лабораторная работа	Содержит 10 лабораторных работ, предусматривающих изучение, тестирование и эксплуатацию лабораторных моделей и измерительных комплексов анализа защиты информации от утечки по техническим каналам.	При успешном выполнении работ в течении семестра фиксируется возможность оценивания только теоретической части в ходе промежуточной аттестации (экзамена), в противном случае, проверка заданий по лабораторным работам выносится на экзамен.

Типовое задание для лабораторной работы

Лабораторная работа №7

«Проверка акустической и виброакустической защищенности помещения с помощью СКМ 21 «Смарт» и ГШ-1»

Цель работы – исследование влияние шума на защищенность помещения от утечки информации по акустическому и виброакустическому каналам.

Задачи, решаемые при выполнении работы:

1. Подготовка к работе СКМ-21.2 (микрофон со штативом, блок СКМ-21.2 и ноутбук) и ГШ-1 в соответствии с п.8 «Подготовка к работе». Они собираются и функционируют отдельно.

2. Проведение спектрального анализа сигналов.

3. Проведение оценки акустического канала утечки информации.

4. Проведение оценки виброакустического канала утечки информации.

5. Анализ полученных результатах с точки зрения защиты от утечки информации поакустическому и виброакустическому каналам.

6. Предложение изменений, которые необходимо произвести, чтобы в данном помещении можно было распространять секретную информацию.

Задания для самостоятельной работы

1. Собрать и подготовить к работе СКМ-21.

2. Провести измерение тестового сигнала.

3. Провести измерение сигнала от источника шума.

4. Провести акустические измерения сигнала на фоне шума.

5. Провести виброакустические измерения сигнала на фоне шума.

6. Провести расчеты отношения сигнал/шум.

7. Построить график спектра шума.

8. Построить график спектра полезного сигнала.

9. Построить график спектра полезного сигнала на фоне шума.

10. Сделать вывод о возможности активной защиты помещения и дать рекомендации по улучшению защиты.

20.2. Промежуточная аттестация

Промежуточная аттестация проводится в соответствии с Положением о проведении промежуточной аттестации при реализации образовательных программ высшего образования ВГУ. Промежуточная аттестация может включать в себя проверку теоретических вопросов, а также, при необходимости (в случае невыполнения в течение семестра), проверку выполнения установленного перечня лабораторных заданий, позволяющих оценить уровень полученных знаний и/или практическое (ие) задание(я), позволяющее (ие) оценить степень сформированности умений и навыков. Для оценки теоретических знаний используется перечень контрольно-измерительных материалов. Каждый контрольно-измерительный материал для проведения промежуточной аттестации включает три вопроса для контроля знаний, умений и владений в рамках оценки уровня сформированности компетенции. При оценивании используется количественная шкала. Критерии оценивания приведены ниже.

Примерный перечень вопросов к экзамену

1. Объекты защиты информации.
2. Случайные антенны.
3. Технические каналы утечки информации. Общая характеристика.
4. Каналы утечки речевой информации.
5. Каналы утечки видовой информации.
6. Каналы утечки информации при передаче ее по каналам связи.
7. Электромагнитное поле побочных электромагнитных излучений.
8. Электромагнитные волны.
9. Ближняя зона излучения электромагнитного поля. Как влияет расстояние от источника излучения до наблюдаемой точки на значения составляющих электромагнитного поля в ближней зоне?
10. Элементарные дипольные излучатели.
11. В каких границах располагается дальняя зона электромагнитного поля?12. Как влияет расстояние от источника излучения до наблюдаемой точки на значения составляющих электромагнитного поля в дальней зоне?
13. Электромагнитные каналы утечки информации ТСПИ.
14. Звуковое поле.
15. Звуковое давление и звуковая мощность. Сила звука.
16. Демаскирующие признаки объекта.
17. Какие демаскирующие признаки характеризуют радиоэлектронные

средства?

18. Пространственно-энергетические характеристики радиоэлектронных средств.
19. Спектральные характеристики радиоизлучений.
20. Спектральные характеристики акустических сигналов.
21. Основные задачи, решаемые пассивными средствами защиты.
22. Основные задачи, решаемые активными средствами защиты.
23. Состав системы обеспечения безопасности объектов.
24. В чем заключается сущность электромагнитного экранирования? Как оценивается эффективность экранирования?
25. Что представляют собой экранированные камеры? Их назначение.
26. С какой целью применяется фильтрация сигналов?
27. Методы пассивной и активной маскировки объектов.
28. Что понимают под аттестационной проверкой?
29. Цель и сущность технического контроля эффективности защиты информации.
30. Методы контроля эффективности защиты информации.
31. Состав нормативной и методической документации на методы испытаний.
32. Задачи эксплуатационного контроля защищенности от утечки по ПЭМИН.
33. Причины и последствия модуляции информационным речевым сигналом высокочастотных колебаний у генераторов технических средств.
34. Какие документы являются нормативно-техническими при проведении аттестации объектов?
35. Какие объекты подлежат обязательной аттестации?
36. Что представляют собой специальные проверки объекта защиты?
37. Какие узлы и устройства ПЭВМ представляют наибольшую опасность утечки информации через ПЭМИН?38. Утечка информации по оптоволоконным каналам связи.
39. Криптографические и случайные методы защиты информации.
40. Квантовая криптография.
41. Состав и назначение прибора «СИГУРД».
42. Состав и назначение прибора «ПИРАНЬЯ».
43. Состав и назначение комплекса «КАССАНДРА».
44. Состав и назначение комплекса «СМАРТ».
45. Перечислить случайные электромагнитные антенны, обнаруженные при проведении лабораторных измерений в помещении.
46. Как практически обеспечить экранирование мобильного устройства связи по электромагнитному каналу?
47. Как практически обеспечить экранирование мобильного устройства связи по акустическому каналу?
48. Перечислить каналы утечки по электромагнитному каналу, обнаруженные при проведении лабораторных измерений в помещении.
49. Перечислить каналы утечки по акустическому каналу, обнаруженные при проведении лабораторных измерений в помещении.
50. Как обнаружить появление нового электромагнитного сигнала с помощью комплекса «КАССАНДРА»?
51. Как обнаружить наличие источников электромагнитного излучения и их тип с помощью прибора «ПИРАНЬЯ».
52. Как осуществить и проверить защиту от утечки информации по акустическому каналу с помощью прибора ГШ-1.
53. Для чего и как используется виброакустический датчик в приборе «ПИРАНЬЯ».

54. В какой зоне излучения (ближней, дальней) легче обнаружить источник и почему?

55. Почему при измерениях прибором «ПИРАНЬЯ» электромагнитного излучения интенсивность сигнала зависит от ориентации антенны? Как это влияет на процедуру измерений?

Пример контрольно-измерительного материала

УТВЕРЖДАЮ
Заведующий кафедрой технологий
обработки и защиты информации
А. А. Сирота
__.__.20__

Направление подготовки: 10.03.01 Информационная безопасность
Дисциплина Б1.О.51 Защита информации от утечки по техническим каналам
Форма обучения: очная
Вид контроля: экзамен
Вид аттестации: промежуточная

Контрольно-измерительный материал № 1

1. Каналы утечки информации при передаче ее по каналам связи.

2. Что представляют собой экранированные камеры? Их назначение.

3. Для чего и как используется виброакустический датчик в приборе «ПИРАНЬЯ».

Преподаватель _____ П.А. Головинский

Критерии и шкала оценивания компетенций (результатов обучения) при промежуточной аттестации

Для оценивания результатов обучения на экзамене используются следующие содержательные показатели (формулируется с учетом конкретных требований дисциплины):

1. знание теоретических основ учебного материала, основных определений, понятий и используемой терминологии;

2. умение проводить обоснование и представление основных теоретических и практических результатов с использованием математических выкладок, блок-схем, структурных схем и стандартных описаний к ним;

3. умение связывать теорию с практикой, иллюстрировать ответ примерами, в том числе, собственными, умение выявлять и анализировать основные закономерности, полученные, в том числе, в ходе выполнения лабораторных заданий;

4. умение обосновывать свои суждения и профессиональную позицию по излагаемому вопросу;

5. владение навыками работы с измерительными приборами и комплексами в рамках выполняемых лабораторных заданий;

6. владение навыками и методиками проведения оценки защиты объектов от утечки информации по техническим каналам.

Различные комбинации перечисленных показателей определяют критерии оценивания результатов обучения (сформированности компетенций) на экзамене: высокий (углубленный) уровень сформированности компетенций; повышенный (продвинутый) уровень сформированности компетенций; пороговый (базовый) уровень сформированности компетенций.

Для оценивания результатов обучения на экзамене используется 4-балльная шкала: «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

Соотношение показателей, критериев и шкалы оценивания результатов обучения на экзамене представлено в следующей таблице.

Критерии оценивания компетенций	**Уровень сформированности компетенций**	**Шкала оценок**
Обучающийся демонстрирует полное соответствие знаний, умений, навыков по приведенным критериям свободно оперирует понятийным аппаратом и приобретенными знаниями, умениями, применяет их при решении практических задач.	Повышенный уровень	Отлично
Ответ на контрольно-измерительный материал не полностью соответствует одному из перечисленных выше показателей, но обучающийся дает правильные ответы на дополнительные вопросы. При этом обучающийся демонстрирует соответствие знаний, умений, навыков приведенным в таблицах показателям, но допускает незначительные ошибки, неточности, испытывает затруднения при решении практических задач.	Базовый уровень	Хорошо
Обучающийся демонстрирует неполное соответствие знаний, умений, навыков приведенным в таблицах показателям, допускает значительные ошибки при решении практических задач. При этом ответ на контрольно-измерительный материал не соответствует любым двум из перечисленных показателей, обучающийся дает неполные ответы на дополнительные вопросы.	Пороговый уровень	Удовлетворительно
Ответ на контрольно-измерительный материал не соответствует любым трем из перечисленных показателей. Обучающийся демонстрирует отрывочные, фрагментарные знания, допускает грубые ошибки	—	Неудовлетворительно

Тесты для проверки остаточных знаний
(могут использоваться при проведении экзамена в дистанционном режиме)

Задания с выбором ответа

1. Акустические закладочные устройства – это

А. специальные миниатюрные электронные устройства перехвата акустической (речевой) информации

Б. специальные миниатюрные электронные устройства для перехвата информации в проводных линиях связи

В. специальные миниатюрные электронные устройства для съема видеоинформации

Г. специальные миниатюрные электронные устройства для съема акустической информации, передаваемой по линиям связи

2. Что такое аудит безопасности компьютерной системы?

А. Инструмент политики безопасности, позволяющий контролировать процесс загрузки системных драйверов

Б. Инструмент политики безопасности, позволяющий отслеживать действия пользователей и системные события и регистрировать их в журнале

В. инструмент политики безопасности, позволяющий наблюдать динамические изменения технического состояния аппаратных компонентов компьютера (температура материнской платы, скорость вращения вентилятора на процессоре и т.д.)

Г. Инструмент политики безопасности, направленный на проверку реализованных в автоматизированной информационной системе процедур обеспечения безопасности с целью оценки их эффективности и корректности.

3. Видимый диапазон длин волн

А. 8 – 14 мкм

Б. 3 – 5 мкм

В. 0,4 – 1,2 мкм

Г. 0,4 – 0,7 мкм

4. Диапазон частот ПЭМИН.

А. 9КГц – 10 ГГц

Б. 20Гц – 20 КГц

В. 300Гц – 300КГц

Г. 2 ГГц – 20ГГц

5. Диапазон частот работы сканирующего приемника ar-8200

А. 50 кГц…1500 МГц

Б. 100 кГц… 1000 МГц

В. 1000МГц … 5200МГц

Г. 500 кГц...2040 МГц

6. Замысел защиты информации – это:

А. основная идея, раскрывающая состав, содержание, взаимосвязь и последовательность осуществления технических и организационных мероприятий, необходимых для достижения цели защиты информации.

Б. деятельность по обеспечению защиты информации не криптографическими методами от ее утечки по техническим каналам, от несанкционированного доступа к ней, от специальных воздействий на информацию.

В. совокупность объекта защиты, физической среды и средства технической разведки, которым добывается защищаемая информация.

Г. реализация конституционных прав человека и гражданина на доступ к информации, на использование информации в интересах осуществления не запрещенной законом деятельности, физического, духовного и интеллектуального развития, а также защита информации, обеспечивающая личную безопасность.

7. Какие виды информации относятся к государственной тайне?

А. Вид секретной информации, содержащей * защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации.

Б. Относятся охраняемые государством сведения в любой области науки, техники, производства и управления, разглашение которых может нанести ущерб интересам государства.

В. Сведения, содержащие коммерческую тайну, адвокатскую и следственную тайну, некоторые виды служебной тайны.

Г. Врачебную тайну, тайну переписки, телефонных переговоров, почтовых и телеграфных отправлений, а также некоторые сведения о частной жизни и деятельности граждан.

8. Защита информации в VPN (виртуальных частных сетях) обеспечивается с помощью

А. межсетевых экранов и шифрования трафика

Б. физической защиты информационных линий связи

В. инкапсуляции и декапсуляции сетевых пакетов

Г. журналирования событий безопасности

9. Защита информации от непреднамеренного воздействия – это

А. защита информации, направленная на предотвращение получения защищаемой информации заинтересованными субъектами с нарушением установленных нормативными и правовыми документами (актами) или обладателями информации прав или правил разграничения доступа к защищаемой информации

Б. защита информации, направленная на предотвращение воздействия на защищаемую информацию ошибок ее пользователя, сбоя технических и программных средств информационных систем, природных явлений или иных нецеленаправленных на изменение информации событий, приводящих к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации

В. защита информации, направленная на предотвращение неконтролируемого распространения защищаемой информации в результате ее разглашения и несанкционированного доступа к ней, а также на исключение (затруднение) получения защищаемой информации иностранными разведками и другими заинтересованными субъектами

Г. защита информации, направленная на предотвращение несанкционированного доступа и воздействия на защищаемую информацию с нарушением установленных прав и (или) правил на изменение информации, приводящих к разрушению, уничтожению, искажению, сбою в работе, незаконному перехвату и копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации

10. Защита информации от НСВ – это

А. защита информации, направленная на предотвращение воздействия на защищаемую информацию ошибок ее пользователя, сбоя технических и программных средств информационных систем, природных явлений или иных нецеленаправленных на изменение информации событий, приводящих к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации

Б. защита информации, направленная на предотвращение получения защищаемой информации заинтересованными субъектами с нарушением установленных нормативными и правовыми документами (актами) или обладателями информации прав или правил разграничения доступа к защищаемой информации

В. защита информации, направленная на предотвращение неконтролируемого распространения защищаемой информации в результате ее разглашения и несанкционированного доступа к ней, а также на исключение (затруднение) получения защищаемой информации иностранными разведками и другими заинтересованными субъектами

Г. защита информации, направленная на предотвращение несанкционированного доступа и воздействия на защищаемую информацию с нарушением установленных прав и (или) правил на изменение информации, приводящих к разрушению, уничтожению, искажению, сбою в работе, незаконному перехвату и копированию, блокированию

доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации

11. Защита информации от НСД – это

А. защита информации, направленная на предотвращение воздействия на защищаемую информацию ошибок ее пользователя, сбоя технических и программных средств информационных систем, природных явлений или иных на целенаправленных на изменение информации событий, приводящих к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации

Б. защита информации, направленная на предотвращение неконтролируемого распространения защищаемой информации в результате ее разглашения и несанкционированного доступа к ней, а также на исключение (затруднение) получения защищаемой информации иностранными разведками и другими заинтересованными субъектами

В. защита информации, направленная на предотвращение получения защищаемой информации заинтересованными субъектами с нарушением установленных нормативными и правовыми документами (актами) или обладателями информации прав или правил разграничения доступа к защищаемой информации

Г. защита информации, направленная на предотвращение несанкционированного доступа и воздействия на защищаемую информацию с нарушением установленных прав и (или) правил на изменение информации, приводящих к разрушению, уничтожению, искажению, сбою в работе, незаконному перехвату и копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации

12. Защита информации от утечки – это

А. защита информации, направленная на предотвращение воздействия на защищаемую информацию ошибок ее пользователя, сбоя технических и программных средств информационных систем, природных явлений или иных нецеленаправленных на изменение информации событий, приводящих к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации

Б. защита информации, направленная на предотвращение получения защищаемой информации заинтересованными субъектами с нарушением установленных нормативными и правовыми документами (актами) или обладателями информации прав или правил разграничения доступа к защищаемой информации

В. защита информации, направленная на предотвращение неконтролируемого распространения защищаемой информации в результате ее разглашения и несанкционированного доступа к ней, а также на исключение (затруднение) получения защищаемой информации иностранными разведками и другими заинтересованными субъектами

Г. защита информации, направленная на предотвращение несанкционированного доступа и воздействия на защищаемую информацию с нарушением установленных прав и (или) правил на изменение информации, приводящих к разрушению, уничтожению, искажению, сбою в работе, незаконному перехвату и копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации

13. Идентификация – это

А. проверка принадлежности субъекту доступа предъявленного идентификатора

Б. установление соответствия реального объекта представленной на него документации, названию во избежание подмены одного объекта другим

В. присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов

Г. совокупность мероприятий по установлению и подтверждению достоверности сведений о пользователях с использованием оригиналов документов и (или) надлежащим образом заверенных копий

14. К какому классу устройств относится устройство AR8200?

А. Индикатор поля.

Б. Сканирующий приемник.

В. Анализатор спектра.

Г. Нет правильных ответов.

15. Какой принцип управления межсетевым экраном предпочтительнее в компьютерной системе, обрабатывающей конфиденциальную информацию?

А. Разрешено все, что не запрещено.

Б. Запрещено все, что не разрешено.

В. Выборочной фильтрации трафика.

Г. Контроля сетевых соединений.

16. Комплекс радиомониторинга и выявления каналов утечки информации «Навигатор» предназначен для решения следующих задач

А. оценки защищенности основных технических средств и систем, предназначенных для обработки, хранения и передачи по линиям связи конфиденциальной информации

Б. оценки защищенности конфиденциальной информации, обрабатываемой основными техническими средствами и системами, от утечки за счет наводок на вспомогательные технические средства, системы и их коммуникации

В. оценки защищенности вспомогательных технических средств и систем, предназначенных для обработки, хранения и передачи по линиям связи конфиденциальной информации

Г. оценки защищенности конфиденциальной информации от утечки по виброакустическому каналу

17. Контроль целостности в системе Secret Net предназначен для

А. слежения за неизменностью контролируемых объектов

Б. выявления НСД

В. выявления вредоносного программного обеспечения

Г. выявления нештатного подключения внешних устройств

18. Межсетевой экран применяется для

А. обнаружения сетевых атак или подозрительных намерений злоумышленника

Б. разграничения доступа между двумя сетями с различными требованиями по обеспечению безопасности

В. контроля почтового трафика и Web-трафика

Г. организации шифрованного сетевого соединения

19. Механизм замкнутой программной среды в системе Dallas Lock 8.0

А. позволяет явно указать с какими программами пользователь может работать

Б. позволят производить разграничение доступа пользователя к настройкам операционной системы

В. позволяет производить блокировку работы пользователя при НСД

Г. позволяет осуществлять кодирование файлов и папок

20. Несанкционированный доступ (НСД) к информации – это

А. доступ к информации, нарушающий установленные правила разграничения доступа, с использованием специально разработанных технических средств

Б. доступ к информации, нарушающий установленные правила разграничения доступа, с использованием штатных средств, предоставляемых средствами вычислительной техники (СВТ) или автоматизированными системами (АС)

В. копирование, искажение или модификация информации с нарушением установленных правил разграничения доступа

Г. совокупность объекта разведки, средства разведки, среды распространения сигнала

21. Параметрический канал утечки информации

А. образуется в результате высокочастотного облучения ОТСС

Б. в результате изменения параметров среды распространения сигнала

В. в результате изменения параметров окружающей среды

Г. в результате высокочастотного облучения ВТСС

22. При индуктивном подключении телефонного закладочного устройства к телефонной линии общее сопротивление

А. возрастет

Б. уменьшится

В. останется без изменений

Г. изменится в соответствии с гармоническим законом

23. Радиозакладочными устройствами называют

А. акустические закладки, передающие информацию по радиоканалу

Б. акустические закладки, передающие информацию по проводным линиям связи

В. акустические закладки, передающие информацию по ИК-каналу

Г. акустические закладки, передающие информацию по ВОЛС-линиям

24. Системы анализа уязвимостей позволяют

А. выявить злоумышленника, работающего в компьютерной сети

Б. выявить уязвимости проектируемой системы защиты информации

В. выявить уязвимости действующей системы защиты информации

Г. выявить уязвимости по результатам журнала аудита безопасности

25. Специальная проверка – это

А. деятельность, заключающаяся в проверке (экспертизе) возможностей юридического лица выполнять работы в области защиты информации в соответствии с установленными требованиями и выдаче разрешения на выполнение этих работ

Б. форма осуществляемого органом по сертификации подтверждения соответствия объектов оценки требованиям по безопасности информации, установленным техническими регламентами, стандартами или условиями договоров. К объектам оценки могут относиться: средство защиты информации, средство контроля эффективности защиты информации

В. исследование, проводимое в целях выявления технических каналов утечки защищаемой информации и оценки соответствия защиты информации (на объекте защиты) требованиям нормативных правовых документов в области безопасности информации

Г. проверка объекта информатизации в целях выявления и изъятия возможно внедренных закладочных устройств

26. Специальное исследование (объекта защиты информации) – это

А. деятельность, заключающаяся в проверке (экспертизе) возможностей юридического лица выполнять работы в области защиты информации в соответствии с установленными требованиями и выдаче разрешения на выполнение этих работ

Б. форма осуществляемого органом по сертификации подтверждения соответствия объектов оценки требованиям по безопасности информации, установленным техническими регламентами, стандартами или условиями договоров. К объектам оценки могут относиться: средство защиты информации, средство контроля эффективности защиты информации

В. исследование, проводимое в целях выявления технических каналов утечки защищаемой информации и оценки соответствия защиты информации (на объекте защиты) требованиям нормативных и правовых документов в области безопасности информации

Г. проверка объекта информатизации в целях выявления и изъятия возможно внедренных закладочных устройств

27. Способ защиты информации – это

А. основная идея, раскрывающая состав, содержание, взаимосвязь и последовательность осуществления технических и организационных мероприятий, необходимых для достижения цели защиты информации

Б. заранее намеченный результат защиты информации

В. совокупность органов и (или) исполнителей, используемой ими техники защиты информации, а также объектов защиты информации, организованная и функционирующая по правилам и нормам, установленным соответствующими документами в области защиты информации

Г. порядок и правила применения определенных принципов и средств защиты информации

28. Какие основные способы разграничения доступа применяются в компьютерных системах?

А. дискреционный и мандатный

Б. по специальным спискам и многоуровневый

В. по группам пользователей и специальным разовым разрешениям

Г. парольное разграничение доступа и иерархическое

29. Учетные записи локальных пользователей в системе Dallas Lock 8.0

А. создаются в системе Dallas Lock только пользователями наделенными соответствующими полномочиями

Б. создаются в операционной системе только пользователями, наделенными соответствующими полномочиями

В. создаются только администраторами безопасности системы Dallas Lock

Г. создаются любым пользователем системы Dallas Lock

30. Цели защиты информации от технических средств разведки

А. предотвращение утечки, хищения, утраты, искажения, подделки информации

Б. предотвращение угроз безопасности личности, общества, государства

В. предотвращение несанкционированных действий по уничтожению, модификации, искажению, копированию, блокированию информации

Г. все перечисленные цели

31. Электрические каналы утечки информации образуются за счет

А. наводок электромагнитных излучений технических средств передачи информации на соединительные линии вспомогательных технических средств связи и посторонние проводники, выходящие за пределы контролируемой зоны

Б. просачивания информационных сигналов в цепи электропитания технических средств передачи информации

В. просачивания информационных сигналов в цепи заземления технических средств передачи информации

Г. все ответы верны

32. Военная разведка

А. занимается сбором сведений, раскрывающих экономический потенциал определенной страны. К таким сведениям относятся характеристики природных ресурсов, промышленности, транспорта, финансовой системы, торговли

Б. направлена на сбор сведений о военном потенциале интересующего ее государства, о новейших образцах военной техники

В. занимается добыванием сведений по новейшим теоретическим и практическим разработкам в области науки и техники

Г. направлена на сбор сведений о новых технологиях

33. Радиотехническая разведка

А. применяется для получения видовой информации о местности и объектах на ней. Бывает наземной и воздушной

Б. представляет собой вид радиоэлектронной разведки по обнаружению и распознаванию радиолокационных станций (РЛС), радионавигационных и радиотелекодовых систем на основе методов радиоприема, пеленгования и анализа радиосигнала

В. основана на использовании лазерных сканирующих камер, которые устанавливаются на воздушных носителях и работают в оптическом диапазоне

Г. применяется во всех диапазонах электромагнитных волн

34. Воздушные каналы утечки информации это

А. среда распространения акустических сигналов являются конструкции зданий, сооружений (стены, потолки, полы), трубы водоснабжения, отопления, канализации и другие твёрдые тела

Б. возникают за счет преобразований акустических сигналов в электрические различными радиоэлектронными устройствами

В. среда распространения акустических сигналов является воздух, а для их перехвата используются миниатюрные высокочувствительные микрофоны и специальные направленные микрофоны

Г. распространение акустических сигналов за пределы контролируемого помещения

35. Электромагнитные каналы утечки информации

А. электромагнитные излучения передатчиков связи, модулированные информационным сигналом (прослушивание радиотелефонов, сотовых телефонов, радиорелейных линий связи)

Б. при подключении к линиям связи

В. эффект возникновения вокруг высокочастотного кабеля электромагнитного поля при прохождении информационных сигналов

Г. эффект возникновения электрических сигналов по действием звуковых колебаний

36. Дипольная антенна

А. линейная антенна малого размера

Б. антенна в форме восьмерки

В. квадратная антенна

Г. малая антенна произвольной формы

37. Магнитная дипольная антенна

А. переменный магнит

Б. излучающий круговой контур малого размера

В. намагниченная дипольная антенна

Г. малая антенна произвольной формы

38. Поле в ближней зоне

А. убывает с расстоянием линейно

Б. убывает обратно пропорционально расстоянию

В. убывает обратно пропорционально квадрату расстояния

Г. убывает по закону экспоненты

39. Электромагнитная волна

А. распространяющиеся в пространстве колебания электрического и магнитного поля

Б. волны колебаний электрического заряда

В. волны в проводниках, помещенных в переменное магнитное поле

Г. волны, вызываемые движением зарядов

40. Наводки электромагнитных излучений ТСПИА.

А. случайно регистрируемые полезные сигналы из контролируемой области.

Б. наводки электромагнитных излучений ТСПИ на соединительные линии ВТСС и посторонние проводники, выходящие за пределы контролируемой зоны

В. изучение ПЭВМ из контролируемой зоны

Г. индуцируемые заряды на поверхностях приборов

41. Параметрический канал утечки информации

А. при воздействии облучающего электромагнитного поля на элементы ТСПИ происходит переизлучение электромагнитного поля

Б. излучение из контролируемой зоны в результате изменения параметров передатчиков

В. излучение высокочастотных генераторов с антеннами, имеющими узкие диаграммы направленности, и специальные радиоприемные устройства

Г. излучение при изменении параметров работающих систем

42. Звуковое поле это

А. способ регистрации акустических сигналов

Б. распределение колебаний давления и плотности в пространстве сплошной среды

В. математический способ описания акустических сигналов

Г. способ исследования утечек по акустическому каналу

43. Скорость звука в воздушной среде

А. 2000 м/с

Б. 300000 м/с

В. 340 м/с

Г. 5000 м/с

44. Скорость электромагнитной волны в вакууме

А. 30000 м/с

Б. 300000 км/с

В. 3000 км/с

Г. 100000 км/с

45. Что такое сферическая волна?

А. волна со сферическим фронтом, на большом расстоянии от источника

Б. волна, идущая от источника сферической формы

В. сферическая компонента волнового поля

Г. разложение поля по сферическим функциям

46. Интенсивность звука измеряется

А. в ваттах (Вт)

Б. в вольтах (В)

В. в децибелах (дБ)

Г. в герцах(Гц)

47. Шум это

А. случайный сигнал с широким спектром

Б. посторонние звуки

В. сигнал, не несущий полезной информации

Г. сигнал с неизвестной кодировкой

48. Звукопоглощающие материалы

А. Отражают звуковые волны.

Б. Преобразуют энергию звуковых волн в тепло.

В. Преобразуют частоту звуковых волн в неслышимый диапазон.

Г. Превращают энергию звуковых волн в электромагнитные волны.

49. Случайные антенны

А. Антенны, которые внесены извне.

Б. Случайно расположенные в контролируемой зоне антенны.

В. Различные предметы, приборы и элементы конструкций, обладающие свойствами антенн.

Г. Антенны, не находящиеся на учете.

50. Явление резонанса

А. Возрастание уровня сигнала при совпадении собственной частоты объекта или прибора с частотой внешнего сигнала.

Б. Явление настройки частоты приемника на частоту передатчика.

В. Согласование двух колебательных процессов.

Г. Совпадение частоты акустических и электромагнитных колебаний.

51. Электродинамические микрофоны.

А. Используют изменение емкости под действием звуковых колебаний.

Б. Основаны на явлении электромагнитной индукции.

В. Работают в результате пьезоэффекта.

Г. Используют изменение электрического сопротивления под действием звуковых колебаний.

52. Направленные микрофоны.

А. Имеют высокую направленность действия для того, чтобы ослабленный звуковой сигнал гарантированно превышал уровень остаточных внешних помех.

Б. Направляются на источник звука.

В. Выстраиваются по периметру зоны разведки.

Г. Имеют чувствительность в определенных частотных диапазонах.

53. Стетоскоп

А. Диффузор с трубками.

Б. Представляет собой вибродатчик, усилитель и головные телефоны.

В. Оптическая система скрытого наблюдения.

Г. Медицинский прибор двойного назначения.

54. Гидроакустический датчик.

А. Для прослушивания акустического сигнала через трубы с водой.

Б. Для контроля за перемещением подводных предметов.

В. Для фиксации опасного повышения давления в гидросистеме.

Г. Для обнаружения нарушения периметра контроля.

55. Телескопический объектив

А. Обеспечивает компактность и скрытость наблюдения.

Б. Обеспечивает возможность наблюдения на больших расстояниях.

В. Обеспечивает возможность складывать оптический прибор при транспортировке.

Г. Обеспечивает скрытость наблюдения.

56. Прибор СИГУРД

А. Обеспечивает контроль СВЧ излучения.

Б. Обеспечивает контроль акустического излучения.

В. Обеспечивает контроль оптического излучения.

Г. Обнаруживает источники инфракрасного излучения.

57. Прибор ПИРАНЬЯ.

А. Портативный прибор контроля акустических полей, электромагнитных полей и наводок.

Б. Прибор постановки шумовых помех.

В. Прибор для прослушивания речевых сигналов.

Г. Прибор для обнаружения визуального наблюдения.

58. Прибор КАССАНДРА.

А. Портативный прибор контроля акустических сигналов.

Б. Прибор для постановки акустических помех.

В. Автоматизированный комплекс анализа электромагнитной обстановки.

Г. Прибор для измерения инфракрасного излучения.

59. Прибор СМАРТ

А. Прибор для анализа электромагнитной обстановки.

Б. Автоматизированный комплекс анализа акустической обстановки.

В. Прибор для обнаружения инфракрасного излучения.

Г. Прибор для постановки акустических помех.

60. Прибор ГШ-1.

А. Генератор акустического шума.

Б. Генератор электромагнитных помех.

В. Источник инфракрасного излучения.

Г. Источник оптического излучения.

Задания с кратким ответом

1. Где эффективнее проводить измерение излучения: в ближней или дальней зоне?

   Ответ: в ближней зоне.

2. На сколько отличается частота соседних октав?

   Ответ: в два раза.

3. Чему равна скорость звука в воздухе?

   Ответ: 340 м/с.

4. Чему равна скорость света в вакууме?

   Ответ: 300000 км/с.

5. В каких единицах измеряется интенсивность звука?

   Ответ: в децибелах

6. Чему равен порог слышимости?

   Ответ: 10^(-12) Вт/м^2.

7. От какого отношения зависит различимость сигнала на фоне шума?

   Ответ: от отношения сигнал/шум.

8. Обладают ли поляризацией звуковые волны?

   Ответ: нет.

9. Могут ли элементы вентиляции быть каналами утечки информации?

   Ответ: да, могут.

10. Может ли металлический шкаф быть резонатором для электромагнитной волны?

    Ответ: да может.

11. Можно ли проводить оценку защищенности объекта от утечек при в процессе его работы?

    Ответ: нет.

12. Какой частотный диапазон использует сотовая связь?

    Ответ: гГц.

13. Как можно считать акустическую информацию с оконного стекла?

    Ответ: лазерным излучением.

14. Являются ли параболические микрофоны направленными?

    Ответ: да.

15. Как называется технология шифрования с использование квантовых методов?

    Ответ: квантовая криптография.

16. Диапазон акустических частот.

    Ответ: 20 Гц * 20 КГц.

17. К каким методам защиты информации относится звукоизоляция?

Ответ: пассивным.

18. При параллельном подключении телефонной закладки к телефонной линии общее сопротивление…

Ответ: снижается.

19. При последовательном подключении телефонной закладки к телефонной линии общее сопротивление…

Ответ: увеличивается.

20. К каким методам защиты информации относится шумоподавление информационного сигнала?

Ответ: активным.

Задания с развернутым ответом

1. Назовите объекты защиты информации.
2. Что называют техническими средствами приема, обработки и хранения информации (ТСПИ)?
3. Приведите определение вспомогательных технических средств и систем (ВТСС).
4. Приведите определение объекта ТСПИ.
5. Приведите определение контролируемой зоны.
6. Что понимают под посторонними проводниками?
7. Приведите определение опасной зоны.
8. Приведите определение белого шума.
9. Приведите определение случайной антенны.
10. Назовите типы случайных антенн.
11. Приведите определение случайной сосредоточенной антенны.
12. Приведите определение случайной распределенной антенны.
13. Что понимают под акустическим каналом утечки информации?
14. Какие составляющие содержит технический канал утечки информации?
15. Назовите основные группы технических каналов утечки информации.
16. Аутентификация это...
17. К электромагнитным относятся каналы утечки информации...
18. Система защиты информации это...
19. Технический канал утечки информации это...
20. Электромагнитный канал утечки информации это...

Критерии оценивания ответа на вопросы с развернутым ответом

Отлично (90-100 баллов) – обучающийся предоставляет правильный полный развернутый ответ с примерами.

Хорошо (70-80 баллов) – обучающийся приводит достаточно полный ответ. Представлены примеры. Допускаются незначительные неточности, нет должной детализации.

Удовлетворительно (50-70 баллов) – представлено основное описание, правильно отражающие основные пункты вопроса и не содержащее грубых ошибок.

Неудовлетворительно (менее 50 баллов) – представлен неполный ответ, содержащий грубые ошибки или неточности.