

Аннотация рабочей программы дисциплины (модуля)
Б1.О.25 Защита информации от утечки по техническим каналам

Целями освоения дисциплины **«Б1.О.26 Защита информации от утечки по техническим каналам»** являются формирование общепрофессиональных компетенций будущих специалистов в области информационной безопасности, формирование у студентов базовых знаний, умений и навыков по основам защиты информации от утечки по техническим каналам достаточных для освоения основной профессиональной образовательной программы направления 10.03.01 Информационная безопасность.

Задачи дисциплины

Основными задачами изучения дисциплины являются:

1. Формирование комплекса базовых навыков по оценке защищенности информации от утечки по техническим каналам; по установке, настройке и эксплуатации аппаратно-программных комплексов для выявления технических каналов утечки информации; по поиску оптимальных решений при проектировании системы защиты информации; по настройке систем управления информационной безопасностью объектов
2. Приобретение навыков применения физических законов и моделей для оценки защищенности информации от утечки по техническим каналам. а также поиску оптимальных решений при проектировании системы защиты информации объекта информатизации.
3. Приобретение навыков использования средства технической защиты информации при установке, настройке и эксплуатации аппаратно-программных комплексов для выявления технических каналов утечки информации и настройке систем управления информационной безопасностью объектов.

Формируемые компетенции и индикаторы их достижения по дисциплине:

Коды компетенции	Содержание компетенций	Код и наименование индикатора достижения компетенции
ОПК-4.	Способен применять необходимые физические законы и модели для решения задач профессиональной деятельности;	ОПК-4.1 - Знает основные физические законы, физическую сущность явлений и процессов; ОПК-4.2 - Умеет использовать математические модели физических явлений и процессов; ОПК-4.3 - Владеет практическими навыками решения типовых прикладных физических задач.
ОПК-6.	Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю;	ОПК-6.1 - Знает основные положения действующих в РФ нормативных правовых актов, нормативных и методических документов по вопросам организации защиты информации ограниченного доступа; ОПК-6.2 - Умеет анализировать и разрабатывать проекты локальных правовых актов, инструкций, регламентов и организационно-распорядительных документов, регламентирующих работу по обеспечению информационной безопасности; ОПК-6.3 - Владеет навыками применения технологий, методов и средств защиты информации

		ограниченного доступа.
ОПК-9	Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности;	ОПК-9.1 - Знает основные понятия криптографии и криптографические методы защиты информации; ОПК-9.2 - Умеет определять наличие типовых технических каналов утечки информации, а также применять методики расчета и инструментального контроля показателей технической защиты информации на объектах информатизации; ОПК-9.3 - Владеет практическими навыками обоснованного выбора и использования СКЗИ при решении задач профессиональной деятельности.
ОПК-4.3	ОПК-4.3. Способен выполнять работы по установке, настройке, администрированию, обслуживанию и проверке работоспособности отдельных программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации автоматизированных систем	ОПК-4.3.1 - Знает основные меры по защите информации в автоматизированных системах, а также содержание эксплуатационной документации автоматизированной системы; ОПК-4.3.2 - Умеет устранять выявленные уязвимости автоматизированной системы, приводящие к возникновению угроз безопасности информации, проводить анализ доступных информационных источников с целью выявления известных уязвимостей, используемых в системе защиты информации программных и программно-аппаратных средств; ОПК-4.3.3 - Владеет навыками осуществления автономной наладки технических и программных средств системы защиты информации автоматизированной системы
ОПК-4.4	Способен осуществлять диагностику и мониторинг систем защиты автоматизированных систем	ОПК-4.4.1 - Знает критерии оценки защищенности автоматизированной системы, технические средства контроля эффективности мер защиты информации; ОПК-4.4.2 - Умеет осуществлять контроль обеспечения уровня защищенности в автоматизированных системах, контролировать события безопасности и действия пользователей автоматизированных систем, а

		также документировать процедуры и результаты контроля функционирования системы защиты информации автоматизированной системы; ОПК-4.4.3 - Владеет навыками оценки защищенности автоматизированных систем с помощью типовых программных средств.
--	--	--

Содержание дисциплины

Тема 1. Введение в техническую защиту информации

Концептуальные основы защиты информации (Стратегия и Доктрина информационной безопасности). Нормативные документы в области ТЗИ. Задача защиты информации.

Тема 2. Технические каналы утечки информации

Каналы утечки информации, обрабатываемой ОТСС. Каналы утечки информации при передаче ее по каналам связи. Каналы утечки информации за счет паразитных связей. Каналы утечки речевой информации

Тема 3. Демаскирующие признаки объектов

Демаскирующие признаки объектов в видимом и инфракрасном диапазоне электромагнитного спектра. Демаскирующие признаки радиоэлектронных средств. Демаскирующие признаки закладных устройств.

Тема 4. Средства выявления каналов утечки информации

Методы автоматизации обнаружения гармонических составляющих тестового сигнала, измерения уровней сигналов, измерения наводок в сети питания, линиях и коммуникациях. Индикаторы электромагнитного поля. Сканирующие радиоприемники, анализаторы спектра, радиочастотомеры. Многофункциональные комплекты для выявления каналов утечки информации. Комплексы для сканирования радиодиапазона. Комплексы измерения побочных электромагнитных излучений и наводок. Локаторы нелинейности. Комплексы измерения характеристик акустических сигналов. Металлодетекторы, портативные рентгенотелевизионные установки, Специальный досмотровый комплект эндоскопов.

Тема 5. Защита информации от утечки по техническим каналам

Скрытие и защита информации от утечки по техническим каналам. Концепция и методы инженерно-технической защиты информации. Пассивное скрытие: экранирование электромагнитных волн, заземление технических средств и подавление информационных сигналов в цепях заземления, фильтрация информационных сигналов. Принцип действия типовых устройств. Способы предотвращения утечки информации через ПЭМИН ПК. Контроль и защита слаботочных и сетевых линий. Скрытие и защита от утечки информации по акустическому и виброакустическому каналам. Скрытие речевой информации в телефонных системах с использованием криптографических методов. Защита конфиденциальной информации в автоматизированных системах: программный комплекс для защиты информации от несанкционированного доступа, программно-аппаратный комплекс «Соболь», применение смарт-карт и USB-ключей, технология Proximity, устройства быстрого уничтожения информации на жестких магнитных носителях.

Тема 6. Методы и средства инженерной защиты информации и технической охраны объектов

Категории объектов защиты. Особенности задач охраны различных типов объектов. Общие принципы обеспечения безопасности объектов Система охранной и пожарной сигнализации. Система контроля и управления доступом. Телевизионные системы

(видеонаблюдение). Периметровая охрана: тепловизионные системы Инфракрасные системы, ёмкостные системы, радиолучевые системы, радиоволновые системы, электрошоковые системы.

Тема 7. Аттестация объектов информатизации по требованиям безопасности информации

Нормативные документы по аттестации объектов информатизации. Стороны, участвующие в аттестации. Приказ ФСТЭК России № 77. Организация работ по аттестации объектов информатизации.

Тема 8. Мероприятия по выявлению и оценке свойств каналов утечки информации

Перечень работ по выявлению каналов утечки информации предусматривает. Специальные проверки. Специальные обследования. Специальные исследования. Специальные исследования акустических и виброакустических каналов. Специальные исследования технических средств и систем на возможность утечки информации за счет ПЭМИН. Специальные исследования акустоэлектрических преобразований.

Тема 9. Технический контроль эффективности мер защиты информации

Цели и задачи технического контроля эффективности мер защиты информации. Порядок проведения контроля защищенности информации на объекте вычислительной техники от утечки по каналу ПЭМИН. Методы испытаний персональных компьютеров. Методы контроля ПЭМИН генераторов технических средств. Порядок проведения контроля защищенности выделенных помещений от утечки акустической речевой информации. Порядок проведения контроля защищенности автоматизированных систем от несанкционированного доступа.

Темы лабораторных занятий

Тема 1. Средства выявления каналов утечки информации.

Тема 2. Защита информации от утечки по техническим каналам

Тема 3. Методы и средства инженерной защиты информации и технической охраны объектов.

Тема 4. Аттестация объектов информатизации по требованиям безопасности информации

Тема 5. Мероприятия по выявлению и оценке свойств каналов утечки информации.

Тема 6. Технический контроль эффективности мер защиты информации.