ЛАБОРАТОРНАЯ РАБОТА № 8

Тема: Технические средства защиты информации.

1. ЗАДАНИЕ К ЛАБАРОТОРНОЙ РАБОТЕ

Предоставить развёрнутый ответ на следующие вопросы:

1.1 Что такое анализатор спектра и зачем он нужен?

1.2 Какие каналы утечки информации существуют?

1.3 Что такое безэховая камера и для чего она нужна?

1.4 Для чего нужны межсетевые экраны?

1.5 Побочные электромагнитные излучения и наводки (ПЭМИН).

1. ТЕОРЕТИЧЕСКАЯ ЧАСТЬ

2.1 Что такое анализатор спектра и зачем он нужен?

Анализатор спектра — прибор для наблюдения и измерения относительного распределения энергии электрических (электромагнитных) колебаний в полосе частот.

Анализатор спектра R&S®Spectrum Rider предназначен для использования в полевых условиях и решения лабораторных задач как внутри, так и вне помещений. Небольшой вес, малые размеры и надёжная конструкция обеспечивают легкость переноски анализатора. Заряда батареи хватает на весь рабочий день. Благодаря подсветке клавиш анализатор может быть использован даже в темноте, а яркий неотражающий дисплей обеспечивает высокий уровень читаемости визуальной информации при ярком солнечном свете. Большие кнопки и многофункциональный поворотный переключатель позволяют работать с прибором, не снимая перчаток. Прибор послужит надежным помощником даже в агрессивных и труднодоступных средах.

FSH — это наиболее выгодный, как технически, так и экономически, анализатор спектра для проведения высокоточных измерений. Он способен выполнять большое количество измерительных функций, необходимых во всем диапазоне проводимых работ: от монтажа и обслуживания базовых станций сети радиосвязи до проверки радиочастотных кабелей и фидерных трактов. Кроме стандартных функций спектроанализатора, FSH-3 способен выполнять измерения КСВ - коэффициента стоячей волны (SWR или VSWR), определять место повреждения РЧ кабели (DTF) и работать в режиме измерения мощности (при подключении датчика измерения мощности).

Основные возможности

* диапазон частот от 5 кГц до 2 ГГц; верхняя предельная частота может быть повышена с помощью программных кодов до 3 / 4 ГГц;
* выдающиеся ВЧ-характеристики;
* идеально подходит для работы в полевых условиях: 8 часов работы от батареи, масса 2,5 кг, подсветка клавиш, быстрая загрузка, антибликовый дисплей, малые габариты, ударопрочный корпус;
* большой цветной дисплей с поддержкой управления сенсорными жестами;
* мастер настройки измерений, поддерживающий составление пользовательских измерительных последовательностей и позволяющий ускорить процесс измерения и предотвратить возникновение операторских ошибок;
* функции и опции для различных областей применения, таких как аэрокосмическая и оборонная промышленность, беспроводные системы связи, теле- и радиовещание, радиочастотные центры и учебные учреждения;
* экономическая эффективность решения за счёт возможности установки программных расширений посредством активации программного ключа;
* стандартная гарантия три года (один год на батарею)

2.2 Какие каналы утечки информации существуют?

Каналы утечки информации — методы и пути утечки информации из информационной системы; паразитная (нежелательная) цепочка носителей информации, один или несколько из которых являются (могут быть) правонарушителем или его специальной аппаратурой.

Виды каналов утечки:

* Акустический канал**.** Акустический канал утечки информации реализуется в следующем:

1. Подслушивание разговоров на открытой местности и в помещениях, находясь рядом или используя направленные микрофоны (бывают параболические, трубчатые или плоские). Направленность 2-5 градусов, средняя дальность действия наиболее распространенных — трубчатых составляет около 100 метров. При хороших климатических условиях на открытой местности параболический направленный микрофон может работать на расстояние до 1 км;
2. Негласная запись разговоров на диктофон или магнитофон (в том числе цифровые диктофоны, активизирующиеся голосом);
3. Подслушивание разговоров с использованием выносных микрофонов (дальность действия радиомикрофонов 50-200 метров без ретрансляторов).

Микрофоны, используемые в радиозакладках, могут быть встроенными или выносными и имеют два типа: акустические (чувствительные в основном к действию звуковых колебаний воздуха и предназначенные для перехвата речевых сообщений) и вибрационные (преобразующие в электрические сигналы колебания, возникающие в разнообразных жестких конструкциях).

* Акустоэлектрический канал. Акустоэлектрический канал утечки информации, особенностями которого являются:
* удобство применения (электросеть есть везде);
* отсутствие проблем с питанием у микрофона;
* возможность съема информации с питающей сети не подключаясь к ней (используя электромагнитное излучение сети электропитания). Прием информации от таких «жучков» осуществляется специальными приемниками, подключаемыми к силовой сети в радиусе до 300 метров от «жучка» по длине проводки или до силового трансформатора, обслуживающего здание или комплекс зданий;
* возможные помехи на бытовых приборах при использовании электросети для передачи информации, а также плохое качество передаваемого сигнала при большом количестве работы бытовых приборов.
* Телефонный канал.Телефонный канал утечки информации для подслушивания телефонных переговоров (в рамках промышленного шпионажа) возможен:
* гальванический съем телефонных переговоров (путём контактного подключения подслушивающих устройств в любом месте абонентской телефонной сети). Определяется путём ухудшения слышимости и появления помех, а также с помощью специальной аппаратуры;
* телефонно-локационный способ (путём высокочастотного навязывания). По телефонной линии подается высокочастотный тональный сигнал, который воздействует на нелинейные элементы телефонного аппарата (диоды, транзисторы, микросхемы) на которые также воздействует акустический сигнал. В результате в телефонной линии формируется высокочастотный модулированный сигнал. Обнаружить подслушивание возможно по наличию высокочастотного сигнала в телефонной линии. Однако дальность действия такой системы из-за затухания ВЧ сигнала в двухпроводной линии не превышает ста метров. Возможное противодействие: подавление в телефонной линии высокочастотного сигнала;
* индуктивный и емкостной способ негласного съема телефонных переговоров (бесконтактное подключение).
* Оптический канал.В оптическом канале получение информации возможно путём:
* визуального наблюдения,
* фото-видеосъемки,
* использования видимого и инфракрасного диапазонов для передачи информации от скрыто установленных микрофонов и других датчиков.

В качестве среды распространения в оптическом канале утечки информации выступают:

* безвоздушное пространство;
* атмосфера;
* оптические световоды.

2.3 Что такое безэховая камера и для чего она нужна?

Безэховая камера (БЭК) — помещение, в котором не возникает эхо. Безэховые камеры бывают следующих видов:

* акустические — в них не возникает отражения звука от стен. Безэховые камеры обычно используются в акустике для имитации неограниченного пространства, в котором ушедшие от источника звуковые волны никогда не возвращаются обратно. В таких камерах проводят измерение (построение) диаграмм направленности излучения (или чувствительности) громкоговорителей (или микрофонов); изучают распределение шумов от промышленных изделий. Иногда в таких камерах проводят запись или прослушивание музыкальных произведений.
* радиочастотные — не возникает отражения радиоволн от стен. Используются для построения диаграмм направленности излучения антенн, изучения электромагнитной совместимости и построения диаграмм ЭПР. Измерения могут проводиться на полноразмерных объектах, включая самолёты, либо на уменьшенных моделях (с соответствующим уменьшением длины волны излучения радара). Радиочастотные безэховые камеры, использующие пирамидальные поглотители радиоволн из пористого материала, отчасти обладают свойствами акустических безэховых камер.

Обычно такие камеры конструируют так, чтобы они ещё и изолировали камеру от внешних сигналов (акустических или радиочастотных). Всё это позволяет производить измерения сигнала, пришедшего непосредственно от источника, исключив отражения от стен и шум извне, сформировав таким образом нахождение источника в свободном пространстве.

2.4 Для чего нужны межсетевые экраны?

Межсетевой экран (МСЭ) — это устройство обеспечения безопасности сети, которое осуществляет мониторинг входящего и исходящего сетевого трафика и на основании установленного набора правил безопасности принимает решения, пропустить или блокировать конкретный трафик.

Межсетевые экраны используются в качестве первой линии защиты сетей уже более 25 лет. Они ставят барьер между защищенными, контролируемыми внутренними сетями, которым можно доверять, и ненадежными внешними сетями, такими как Интернет.

Межсетевой экран может быть аппаратным, программным или смешанного типа.

Среди задач, которые решают межсетевые экраны, основной является защита сегментов сети или отдельных хостов от несанкционированного доступа с использованием уязвимых мест в протоколах сетевой модели OSI или в программном обеспечении, установленном на компьютерах сети. Межсетевые экраны пропускают или запрещают трафик, сравнивая его характеристики с заданными шаблонами.

Наиболее распространённое место для установки межсетевых экранов — граница периметра локальной сети для защиты внутренних хостов от атак извне. Однако атаки могут начинаться и с внутренних узлов — в этом случае, если атакуемый хост расположен в той же сети, трафик не пересечёт границу сетевого периметра, и межсетевой экран не будет задействован. Поэтому в настоящее время межсетевые экраны размещают не только на границе, но и между различными сегментами сети, что обеспечивает дополнительный уровень безопасности.

2.5 Побочные электромагнитные излучения и наводки (ПЭМИН).

Угрозу хищения информации путем ее утечки создают сигналы, случайно возникающие в результате побочных электромагнитных излучений и наводок (ПЭМИН). Эти сигналы называют также опасными.

Источниками опасных для безопасности информации сигналов являются радио и электротехнические элементы и устройства в принципе любых радиоэлектронных и электрических устройств и приборов. В некоторых средствах звукозаписи, звукофикации и передачи информации предусматриваются дополнительные меры по безопасности информации, исключающие появление опасных сигналов. Однако технические меры по защите информации существенно повышают стоимость этих радиоэлектронных средств и делают их неконкурентными на рынке. Поэтому основной тенденцией предотвращения утечки информации из незащищенных радиоэлектронных средств является применение дополнительных средств защиты информации.

Радиоэлектронные и электрические средства и системы, содержащие потенциальные источники опасных сигналов, разделяют на основные и вспомогательные. Основные средства и системы обеспечивают обработку, хранение и передачу защищаемой информации, вспомогательные технические средства и системы (ВТСС) - остальные.

Несмотря на многообразие типов средств источники опасных сигналов можно классифицировать исходя из их физической природы следующим образом:

- акустоэлектрические преобразователи;

- излучатели низкочастотных сигналов;

- излучатели высокочастотных сигналов;

- паразитные связи и наводки.

Побочные излучения — это радиоизлучения, возникающие в результате любых нелинейных процессов в радиоэлектронном устройстве, кроме процессов модуляции. Побочные излучения возникают как на основной частоте, так и на гармониках, а также в виде их взаимодействия. Радиоизлучение на гармонике — это излучение на частоте (частотах), в целое число раз большей частоты основного излучения. Радиоизлучение на субгармониках — это излучение на частотах, в целое число раз меньших частоты основного излучения. Комбинационное излучение — это излучение, возникающее в результате взаимодействия на линейных элементах радиоэлектронных устройств колебаний несущей (основной) частоты и их гармонических составляющих.

Любая передача электрического сигнала сопровождается электромагнитным излучением. Если электромагнитный сигнал сам не используется как носитель информации (радиоволны), то подобное излучение оказывается крайне нежелательным с точки зрения безопасности.

Осознание опасности побочных электромагнитных излучений привело к тому, что в наши дни правительственные службы используют дорогое металлическое экранирование отдельных устройств, помещений, а иногда и отдельных зданий. Однако даже для внутренних экранированных помещений существует принцип разделения оборудования на так называемое «красное» и «черное». «Красное» оборудование, используемое для обработки конфиденциальной информации (например, мониторы), должно быть изолировано фильтрами и экранами от «черного» (например, радиомодемов), которое передает данные без грифа «секретно».

«Оценочно, по каналу ПЭМИН (побочных электромагнитных излучений и наводок) может быть перехвачено не более 1-2 процентов данных, хранимых и обрабатываемых на персональных компьютерах и других технических средствах передачи информации (ТСПИ)». На первый взгляд может показаться, что этот канал действительно менее опасен, чем, например, акустический, по которому может произойти утечка до 100% речевой информации, циркулирующей в помещении. Однако, нельзя забывать, что в настоящее время практически вся информация, содержащая государственную тайну или коммерческие, технологические секреты, проходит этап обработки на персональных компьютерах. Специфика канала ПЭМИН такова, что те самые два процента информации, уязвимые для технических средств перехвата - это данные, вводимые с клавиатуры компьютера или отображаемые на дисплее, то есть, парадоксально, но весьма значительная часть сведений, подлежащих защите, может оказаться доступна для чужих глаз.

Традиционно считается, что перехват ПЭМИН и выделение полезной информации - весьма трудоемкая и дорогостоящая задача, требующая применения сложной специальной техники.

**ВЫВОДЫ**

В ходе проведения лабораторной работы были изучены технические средства защиты информации, а также проверена их работа на практике.