**Государственное бюджетное профессиональное образовательное учреждение**

**Новосибирский Колледж Почтовой Связи и Сервиса**

**Выпускная квалификационная работа на тему:**

**« Организация сети WF с регистрацией»**

**Выполнил студент группы ТС-43**

**Фокин Даниил Александрович**

**Шабронов А.А.**

**Новосибирск 2020**

**Содержание**

# **Введение**

Знание как правильно получить доступ к защищенной информации – обязательное условие для специалистов в рабочей области информационной безопасности . Для того чтобы охранять информацию нужно знать , как взламывают и получают её злоумышленники . Научиться создавать специальные каналы . И сейчас мы в этом подробно разберемся.

# **1.1. Классификация электромагнитных каналов утечки информации**

Электромагнитные волны имеют важное значение для передачи информации. Их можно передавать как на сотни метров , так и на сотни тысяч километров . Утечка информации по радиоканалу происходит посредством перехвата электромагнитных излучений диапазона , которые передаются от отправителя к адресату. Также можно осуществить взлом сигналов у радиолокационных и радионавигационных сис­тем, радиостанций и систем связи ,систем телеуправления, средств радиотелефонной связи, мониторов ПЭВМ, радиозакладок различного типа, перегово­ров внутри помещений предприятия с помощью беспровод­ных служебных систем связи и пр.

Перехват информации по радиоканалам имеет ряд плюсов по сравнению с другими каналами утечки информа­ции, а именно:

– отсутствует естественный контакт с источником информации;

– на прием сигналов не влияет время года и время суток;

– информация поступает в реальном времени;

– перехват информации осуществляется достаточно незаметно ;

– у источника информации нету сведений о начатом процессе перехвата;

– дальность перехвата ограничивается только некоторыми особенно­стями распространения соответствующего диапазона радио­волн и возможностями источника информации.

Утечка информации по радиоканалу может происходить как без преобразования информационного сигнала, так и с его участием.

В технических средствах генерирования, распростране­ния и приема электромагнитных волн используется большое количество функциональных элементов.

#### **1.2. Перехват сигналов связных радиостанций**

Электромагнитные излучения передатчиков свя­зи, модулированные информационным сигналом, могут пере­хватываться прямым образом с использованием дефолтных тех. средств.

Упрощенная структура типового комплекса средств пере­хвата сигналов связных радиостанций включает:

– *приемные антенны.* Они нужны для изменения электромагнитной волны в электрические сигналы, амп­литуда, частота и фаза которых соотносится аналогичным характеристикам электромагнитной волны;

– *радиоприемник.* Предоставляет поиск и селекцию ра­диосигналов по частоте, усиление и демодуляцию выделенных сигналов, их усиление и обработку;

– *анализаторы технических характеристик сигна­лов.* Определяются параметры сигналов: частотные, времен­ные, энергетические, виды модуляции, структуру кодов и др.;

– *радиопеленгатор.* Позволяет найти направле­ние на источник электромагнитного излучения и его коор­динаты;

– *регистрирующее устройство.* Поставляет запись сигналов для документирования и последующей обработки.

Для перехвата радиосигналов связных радиостанций используют разные виды приемников или радиокомп­лексы.

Так, например, используются приемные устройства AR-3000A, AR-5000, АРК-ЦТ, Winradio 3100i-DSP, радиокомп­лексы OSC-5000, AFK-MK1, АРК-Д1, АРК-ПК-П, R9000-DM-20 (профессиональный радиоприемник – многофункциональ­ный комплекс).

#### **1.3. Перехват радиотелефонных сигналов**

Для перехвата радиосигналов с довольно-таки тяжелой структурой, которая применятся в сотовой или пейджинговой , а также в других видах мо­бильной связи, созданы уникальные принимающие комплексы.

Например, система контроля и использования служебных ра­дио­те­ле­фо­нов сотовой связи стандарта NMT-450 ТТС-1 (фир­ма "Нелк") дает возможность находить и даже позволяет следовать по часто­те исходящие и входящие звонки абонентов мобильной связи, приводить в исполнение отслеживание по частоте за каналом во время разговора по мобильному телефону, вести одновременно авто за­пись разговора на диктофон и т.п. В комплексе используются ПЭВМ и два приемника AR 3000 А.

Для отслеживания текстовых сообщений мобильных телефонов созданы ав­томатизированные станции по перехвату сотовых систем связи. В состав этих станций входят: переносной компьютер, спецдемо­дулятор, принимающее устройство, управляемое компьютером. Нужно просто на экране машины задать номер интересую­щего вас абонента – и комплекс начнет сразу автоматически записывать входящие разговоры , также определять номера звонящих абонентов  к абоненту за которым мы наблюдаем , следить за мобильным объектом при переходе из соты в соту.

Похожие системы есть и для радиотелефонов российской системы "Алтай".

Культивация перехваченного радиосигнала используется с помощью средств тех. анализа. К ним относятся: Stabilock 4051, Stabilock 4032, HP 8920 A/D и др.

Для перехвата типографических передач применяются спе­циальные комплексы типа FAX MANAGER, ФАКС-02, 4600-FAX-INT, и др. Они нужны для того чтобы обеспечить автоматическим перехватом в настоящем времени абсолютно любого числа страниц, которые переда­ются по факс-машине со скоростью от 330 до 9700 бит/с, запись текстового сообщения и служебной информации, вывод их на печать.

Перехват пейджинговых передач происходит с помощью спец. комплек­сов .

Например, разработаны АРК-ПК , АРК-Д1 с использованием программного обеспечения (ПО) СМО-ДЕМ, которое выполняет следующие задачи:

– программное обеспечение , которое настроит приемник на нужные нам частоты, заблаговременно занесённые в файл пейджерных радиостанций;

– прием сообщений, которые передаются в формате PJCSAG со скоростью передачи от 512 до 2400 Бод;

– авто распознавание скорости и полярности передачи;

– регистрация в реестре сообщений, руч­ное декодирование и анализ принятых нами сообщений, мгновенный просмотр полученных сообщений, поиск нужного сообщения по шаблону ;

– запоминание и накопление в базе данных информации об абонентах и ее обновление;

– прием сообщений абсолютно всех абонентов (режим "Обнаруже­ние");

– сохранение содержимого экрана в файле.

####  **1.4. Радиомаяки**

Позволяют осуществлять перехват нужной информации о составе технических средств и местах их установки. Такая информа­ция является очень важной, так как позволяет установить, какие средства обработки и передачи информации устанавливаются в помещениях контролируемой зоны. Кроме того, покупаемая и устанавливаемая техника может обеспечивать заклад­ные устройства, управляемые на расстоянии , то есть дистанционно. Подготовка по организации канала утечки информации содержит в себе и процеду­ру локализации "меченых" тех. средств. Для нужно использовать радиосигнальные маяки.

Радиосигнальные маячки могут устанавливаться , например, в упаковку какого-либо продукта , что позволяет контролировать места размещения закупленных средств вычислительной техники. В системный блок могут встраиваться доп. устройства, которые создаются из стандартных модулей, применяемых в ПК, и прячутся таким образом, чтобы иметь доступ к воспроизводимой или вводимой информации.

Передача на пункт прослушивания , конечно же осуществляется по ра­диоканалу.

#### **1.5. Радиозакладки**

Большой ассортимент видов информационных сигналов заставило создавать и выпускать большое количество различных закладок, обеспечивающих преобразование исходных ин­формационных сигналов в радиоизлучение. Для этих преоб­разований можно использовать различные сочетания ФЭ.

В качестве источников питания закладных устройств также можно использовать электрические цепи:

– теле­фонной линии за счет гальванического подключения или ис­пользования специальных сетевых блоков питания;

– силовой, осветительной сети;

– термоэлектрических генераторов;

– детекто­ров СВЧ-энергии.

Также закладное устройство может использовать свой источник питания : радиоизатопную батарею и другие химические источники.

Выбор источника питания обусловливается местом , куда мы будет ставить наш радиомаячок . Наиболее популярны радиозакладки по типу , радиомикрофонов ( чтобы прослушивать перехваченную информацию ) .

***Радиомикрофоны.*** Радиомикрофоны хороши тем , что у них довольно таки простая конфигурация , плюс дешевые комплектующие для их создания , ну и конечно крохотные размеры .Радиомикрофоны существуют непрерывного действия ,управляемые дистанционно , а также с системой VOX (то есть когда появляется речевой сигнал , микрофон включается и начинает записывать).

Микрофоны состоят из: модуля передатчика , выносной антенны , блока питания и микрофона.

Благодаря своей чувствительности, такие микрофоны спокойно могут обхватывать зону в 20 м2.При маскировки такого микрофона, делают отверстие от 3 до 5 мм. В основном почти все такие радиомикрофоны работает в диапазоне от 300 до 500 мГц. В таком диапазоне легче удается достичь приемлемых характеристик для прохождения радиосигнала. Выходная мощность передатчика находится из условий использования и требуемой дальности. Чаще всего в радиомикрофонах используются гибкие внешние антенны , выглядят как отрезок многожильного провода , длинною в четверть волны .

Сетевые блоки дают возможность использовать радиомикрофоны неограниченное время , т.к. питание подается от телефонных или других электрических сетей .

Места где обычно устанавливают радиомикрофоны:

– электрические розетки и выключатели;

– телефонный аппарат;

– горшочки и вазы для цветов;

– письменные приборы;

– мебель (столы, стулья, шкафы, зеркала);

– бытовые приборы (чайники, телевизоры, обогревате­ли, приемники, таймеры);

– элементы конструкции здания (вентиляционные сис­темы, батареи отопления);

– системы электрических соединений (распределитель­ные устройства, коробки);

– предметы интерьера (картины, шторы).

Частенько такие микрофоны маскирую, чтобы было еще тяжелее найти, а маскируют под все что угодно , например : под предметы быта или же оргтехнику.

Рассмотрим некоторые типы таких микрофонов.

**РМК061*.***Данная конструкция выглядит как ,

прямоугольная платка 23х9х6 мм, залитая герметиком со встроенным микрофоном , удобную гибкую антенну и выходы для подключения к питанию от 3 до 6 В.

Этот радиомикрофон является чуть ли не классикой у злоумышленников , поскольку он универсален , также он содержит кварцевый стабилизатор . Прием сигналов от радиоприемника можно осуществить с помощью спец. приемников или сканеров с частотной широкополосной модуляцией частоnы , этот режим называется WFM .

**РМК191.** Этот радиомикрофон создан для того чтобы скрытно размещать его на одежде , например под галстуком .Не обязательно выносить его на улицу , т.к. зона прямой видимости составляет целых 100 метров , а работает без прямого питания около 3 часов .

Существуют и по серьёзней микрофоны например: РК-260 ( без прямого питания работает около 750 часов ) , РК-270 ( только вдумайтесь он работает без питания целый год !) , есть микрофон РК 575 он выглядит как обычная зажигалка , или же РК 585 он выглядит как простая шариковая ручка , а есть в виде гвоздя это РК 520 ; и таких микрофонов огромное количество . Такие радиомикрофоны становятся все совершеннее и все менее заметнее, также стараются повысить зону для дистанционного управления.

***Другие типы радиозакладок.*** Также для взлома электронных сигналов устанавливают специальные закладки в накопители информации ( которые работают на магнитных дисках ), также могут установить в клавиатуру (для вывода информации , например какого-нибудь пароля) и в самом системный блок . Такие закладки очень противные , во-первых их трудно найти , во-вторых они могут месяцами питаться от источников напряжение вычислительной технике и могут передавать информацию на 2 км .

Для съема электрических сигналов созданы специальные закладки , по типу SIPE 005, НВ-ПТ ( выгладит как конденсатор ).

 Для съема акустической информации по виброакустиче­скому каналу созданы хитрые и уникальные радиостетоскопы: STG 4025 (пе­редатчик-стетоскоп, дальность 250 м, масса 18 г) STG 4027(передатчик-стетоскоп, дальность 200 м, масса 25 г) , AD-50 (радиостетоскоп, дальность 100 м, масса 120 г), РК 1005 (пере­датчик-стетоскоп, дальность 500 м, масса 13 г).

Для того чтобы снять видеосигнал созданы специальные видеокамеры с передачей изображения по радиоканалу . А для снятия оптических сигналов с волоконных линий связи , созданы закладки с перехватом нужной информации с помощью светодиодов.

### **2. Электромагнитные явления и эффекты в образовании каналов утечки информации.**

#### **2.1. Источники электромагнитных излучений и наводок.**

Электрическая аппаратура и электрические системы различ­ного применения, интегральные схе­мы, вычислительная техника, электровакуумные приборы и другие элементы когда работают создают в окружающем пространстве эл. поля. Эти поля могут сделать элект­ромагнитные , скажем так, «наводки» в располагающихся неподалеку силовых, слаботочных и осветительных сетях, элемен­тах и цепях охранной и пожарной сигнализации, телефонных линиях , приемниках электромагнитных излучений и других электрических и элект­ронных системах. Электромагнитные излучения и их наводки – это результат проявления ряда ФЭ(функционального эффекта):эффекта индукции и взаимоиндукции, эффекта возникновения маг­нитного поля вокруг проводника при протекании по нему электрического тока ,эффекта взаимодействия электрических зарядов, эффекта возникновения резонанса в электричес­ких цепях, эффекта су­перпозиции, эффекта электропроводимости и магнитопроводимости, эффекта магнитострикции и др.

Дополнительные эл. излучения и наводки (ПЭМИН) от тех. средств различного назначения позволяют содержать защищаемую информацию. В этом случае они начинают пре­вращаться в источники опасных сигналов.

Перехват дополнительных эл. излучений и наво­док обеспечивает добычу информации, содержащуюся не­посредственно в формируемых, передаваемых или отображае­мых (телеграфных, телеметрических, телефонных и др.) сообщениях и документах (разных текстах, различных таблицах; рисунках, картах, снимках, телевизионных изображениях и т.д.), с исполь­зованием электронной радиоаппаратуры, записывающие эл. излучения и электрические сигналы, которые наводятся первичными эл. излучениями в токопроносящих цепях разных тех. оборудования и конструкциях зданий.