Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования «Тульский государственный университет»
Институт прикладной математики и компьютерных наук

Кафедра «Информационная безопасность»

КУРСОВАЯ РАБОТА

по дисциплине

«Физические основы защиты информации»

на тему

«Физические эффекты, которые могут стать основой физической утечки информации»

Выполнила: ст. гр. 230711 _____ (подпись) Павлова В. С.

Проверил: д. т. н, доц. каф. ИБ _____ (подпись) Токарев В. Л.

Тула, 2023

ЗАДАНИЕ

на курсовую работу по дисциплине

«Физические основы защиты информации»

студента гр. 230711 Павловой Виктории Сергеевны

Тема курсовой работы

«Физические эффекты, которые могут стать основой физической утечки информации»

Исходные данные

«Проводные телефонные каналы утечки информации»

Задание получил _____ _____
(ФИО) (подпись)

Задание выдал _____ _____
(ФИО) (подпись)

Дата выдачи задания 21.02.2023 г.

График выполнения КР 21.02-28.02 – Получение и ознакомление с заданием

01.03-22.03 – Изучение литературы и других исходных материалов

23.03-03.05 – Изучение теории, раскрывающей тему курсовой работы

04.05-17.05 – Реализация практической части курсовой работы

18.05-24.05 – Анализ результатов

25.05-07.06 – Оформление пояснительной записки и сдача на проверку

29.06.2023 – Защита курсовой работы

Рекомендации и особые отметки _____

«__» _____20__г

Содержание

Введение

Реалиям настоящего времени свойственно стремительное развитие технологий и возрастающий объём обмена информацией, что делают защиту от утечек необходимой задачей для всех организаций. Сохранение конфиденциальности информации в условиях угроз безопасности и защита от утечек информации на сегодняшний день является одной из ключевых задач кибербезопасности.

Несмотря на то, что на данный момент существует множество способов передачи информации, проводные телефонные каналы по-прежнему остаются важным средством связи в различных сферах жизни. Существуют опасности, связанные с возможностью утечки информации через эти каналы. Физические эффекты, которые могут стать основой физической утечки информации, могут быть использованы злоумышленниками для доступа к конфиденциальной информации и её перехвата. В связи с этим проблема защиты телефонных каналов от утечки информации и на сегодняшний день является актуальной и требует внимания. В данной курсовой работе будут рассмотрены основные пути утечки информации через телефонные каналы, а также существующие способы защиты от этих утечек.

Целью данной курсовой работы является изучение физических аспектов работы проводного телефона и телефонных каналов связи, которые могут стать уязвимостями (источниками возможности перехвата информации) при передаче сигналов, а основной поставленной задачей является изучение и анализ методов защиты телефонных каналов связи.

I. Физические аспекты работы телефонного канала

1.1 Телефонный аппарат и физика его работы

Телефонный аппарат – это устройство, которое, физический принцип работы которого основан на преобразовании звуковых колебаний в электрические сигналы, которые передаются по проводам и восстанавливаются в звуковые колебания на другом конце линии. Основными элементами аппарата, как показано на рисунке 1, являются микрофон и приёмник, которые преобразуют звуковые колебания в электрические сигналы и наоборот [1].

Рисунок 1 – Устройство и принцип работы телефонного аппарата

Упрощённо основные этапы работы телефонного аппарата можно сформулировать так:

- голосовой сигнал, сформированный динамиком в трубке, преобразуется в звуковые колебания, распространяющиеся по воздуху;
- колебания попадают в микрофон телефонной трубки, который преобразует их в электрические сигналы;
- электрический сигнал передается через проводную линию до телефонного аппарата абонента, где происходит обратный процесс;
- сигнал поступает в динамик, который преобразует электрические сигналы в звуковые колебания.
- звуковые колебания передаются в воздух и слышимы абонентом, который находится на другом конце линии.

Разумеется, на практике устройство телефонных аппаратов, особенно современных, более сложное и включает в себя и другие элементы, например, противоместные схемы, элементы, компенсирующие потери во время передачи по телефонной линии и т.п. Это можно заметить на примере телефонного аппарата ТА-72М-5, предназначенного для работы в городских сетях, схема которого приведена на рисунке 2. Его коммутационно-вызывную часть образуют рычажный переключатель SA_1, звонок HA_1, разделительный конденсатор C_1 и номеронабиратель SA_2. Разговорная часть телефонного аппарата состоит из телефона BF_1, микрофона BM_1, трансформатора T_1, балансного контура (конденсаторы C_1 и C_2, резисторы R_1-R_3) и ограничительных диодов VD_1, VD_2. Разговорная часть выполнена по противоместной схеме мостового типа [2].

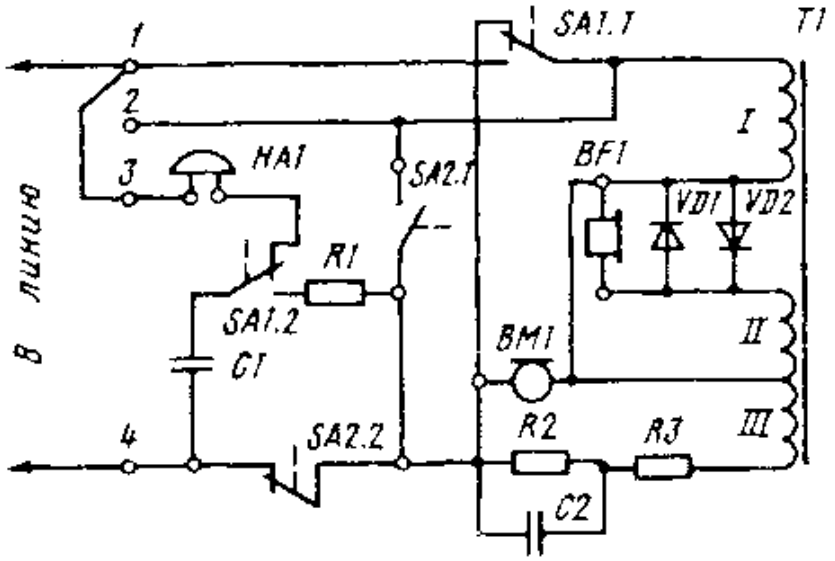

Рисунок 2 – Схема простейшего телефонного аппарата на примере ТА-72М-5

Когда трубку телефона поднимают, происходит замыкание цепи между проводами телефонной линии и включение тока, который вызывает срабатывание электромагнита в телефонной трубке. Это приводит к тому, что мембрана в трубке начинает колебаться в соответствии с звуковыми волнами, создаваемыми голосом человека. Когда звуковые волны попадают на мембрану, она создает колебания воздуха, которые в свою очередь передаются по телефонной линии.

На другом конце телефонной линии сигнал поступает на электронное устройство, которое воспроизводит голосовой сигнал через динамик. В то же время, когда человек говорит, микрофон в телефонной трубке преобразует звуковые колебания в электрические сигналы, которые передаются через телефонную линию.

В проводных телефонных каналах используется аналоговая модуляция для передачи информации. Электрические сигналы, представляющие звуковые колебания, изменяют амплитуду высокочастотного сигнала, который передается по проводам. Для обеспечения качественной передачи сигнала используется усиление сигнала перед передачей и фильтрация шумов на принимающей стороне.

1.2 Основные характеристики телефонных каналов

Рассмотрим некоторые характеристики телефонной линии. На рисунке 3 приведена схема цепи прохождения постоянного тока через абонентские катушки, линию и телефонный аппарат. Напряжение батареи на большинстве АТС (автоматизированных телефонных станциях) в нашей стране составляет $U_б = 60$ вольт, но может колебаться в пределах 24-100 вольт. [3]

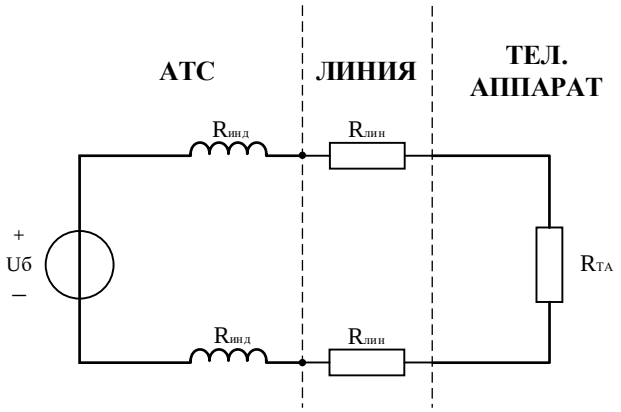

Рисунок 3 – Цепь постоянного напряжения и постоянного тока через абонентские катушки, линию и телефонный аппарат

Нетрудно рассчитать, что величина тока, с учётом сопротивления нагрузки $R_{\text{нагр}} = 2900$ Ом (включает в себя последовательно подключённые сопротивления: катушек $R_{\text{инд}} = 400$ Ом каждая, линии, составляющее $R_{\text{линии}} = 1800$ Ом и самого телефонного аппарата $R_{\text{ТА}} = 300$ Ом), минимальный ток линии $I = \frac{U_{\text{б}}}{R_{\text{нагр}}} = \frac{60\text{ В}}{2900\text{ Ом}} = 20{,}7 \approx 20$ mA.

В приложении в таблице 1 более подробным образом с опорой на информацию из ГОСТ 7153-85 сформулированы основные характеристики электрических параметров телефонных аппаратов, а в таблице 2 приведены характеристики сигналов, поступающих от АТС к абонентскому устройству.

Сама же телефонная линия, с физической точки зрения, представляет собой пару медных проводов, обычно диаметром $d = 0{,}5 - 1$ мм, закрытых в изоляционной оболочке. Эти провода соединяют телефонный аппарат с центральным офисом, который занимается коммутацией вызовов и передачей голосовой информации через линию. Внутри телефонной линии течет электрический ток, который создает электромагнитное поле вокруг линии. Для передачи голоса по телефонной линии используется метод модуляции амплитуды, при котором изменения амплитуды тока соответствуют изменениям амплитуды голосового сигнала. Кроме того, используется также метод частотной модуляции, при котором изменения частоты тока соответствуют изменениям частоты голосового сигнала. [3]

Обобщая, можно сказать, что ***телефонная линия*** – это физический канал, через который передается голосовая информация, и, следовательно, который может быть подвержен утечке информации.

1.3 Источники физической утечки информации телефонного канала

Характеристики проводных телефонных каналов могут варьироваться в зависимости от многих факторов, таких как длина линии связи, качество проводов и их диаметр. Например, медные провода, которые широко используются для передачи голосовой и цифровой информации, обладают

хорошими электрическими характеристиками и имеют достаточно высокую скорость передачи данных. Однако, если рассматривать их с точки зрения физической информационной безопасности, они подвержены влиянию электромагнитных помех и могут быть уязвимы к перехвату информации.

Существуют также оптоволоконные линии связи, обладающие высокой скоростью передачи данных. Их можно считать более безопасными, так как они не излучают электромагнитные волны и не могут быть подвержены перехвату информации посредством электромагнитных помех. Однако, такие линии обычно дороже и сложнее в установке и подключении [3].

Среди уязвимостей, которые могут послужить основной физической утечки информации по проводному телефонному каналу связи можно выделить следующие [4]:

1. Проводные кабели

Кабели, по которым передаются сигналы в телефонной сети, могут быть подвержены механическому воздействию, что может привести к искажению сигнала или даже его полной потере. Кроме того, кабели могут быть перехвачены и подключены к устройствам, например, средствам подслушивания.

2. Разводка и соединения

Как и любые электрические цепи, проводные телефонные каналы могут быть подвержены коротким замыканиям, ослаблению сигнала или даже его полной потере из-за плохой разводки или соединений. Кроме того, неправильное подключение устройств, например, злоумышленником, может привести к возможности перехвата информации.

3. Электромагнитные помехи

Электромагнитные поля, возникающие вблизи электрических устройств, могут вызывать помехи в работе телефонной связи. В частности, такие помехи могут привести к искажению сигнала, что делает его уязвимым к перехвату.

4. Утечки сигнала

Сигнал, передаваемый по проводной телефонной линии, может утечь на другие провода или даже на землю. Это может привести к возможности перехвата информации, особенно в случае использования неэкранированных кабелей.

5. Подслушивание

Злоумышленник может установить устройство для подслушивания телефонного разговора. Например, это может быть микрофон, установленный в телефонной трубке или проводе, или специализированное устройство, подключенное к линии.

II. Основные методы перехвата информации через телефонный канал

2.1 Классификация методов воздействия на телефонные линии

Основываясь на физических принципах устройства телефонных линий связи и непосредственно самих телефонных аппаратов, приведённых в предыдущей главе данной курсовой работы, можно выделить следующие виды утечек информации через телефонный канал:

1. ***Акустический метод***: используется для записи звуков, производимых во время телефонного разговора, с помощью специальных устройств, которые устанавливаются непосредственно на телефонных линиях.
2. ***Метод компрометации устройств***: заключается в том, что злоумышленник вносит изменения в аппаратуру или программное обеспечение, чтобы перехватывать информацию;
3. ***Визуальный метод***: непосредственное наблюдение за действиями пользователя и аппаратурой (например, видеосъёмка);
4. ***Электромагнитный метод***: заключается в использовании электромагнитных полей и наводок для перехвата информации, передаваемой по телефонной линии;
5. ***Метод перехвата радиосигналов***: используется для перехвата радиосигналов, которые передаются между устройствами, которые подключены к телефонной линии;
6. ***Физический метод***: заключается в использовании физических средств для проникновения в помещение, где находится телефонная линия, и установки устройств для перехвата информации;

Далее рассмотрим несколько конкретных методов, имеющих наибольшее распространение и опасность. Согласно статистике, предоставленной компанией Verizon в ее отчете о безопасности, 35% всех нарушений информационной безопасности в 2019 году были связаны с использованием физических методов атаки, включая непосредственное подключение к телефонной линии и установку

устройств наблюдения внутрь телефонного аппарата. Высокочастотное навязывание было использовано в 4% случаев, но часто вело к серьезным последствиям, таким как утечка конфиденциальной информации или потеря денег [6].

2.2 Метод высокочастотного навязывания

Высокочастотное навязывание – (англ. High-Frequency Trading) – это метод, который заключается в использовании радиочастотных сигналов для передачи информации через телефонную линию. Суть метода в том, что на передаваемый сигнал накладывается дополнительный шум высокой частоты, который затрудняет его перехват и декодирование [4]. Для кодирования информации в виде высокочастотного сигнала, который накладывается на основной сигнал, используется ***модуляция***. Этот дополнительный высокочастотный сигнал создает шум, что делает его перехват и декодирование затруднительным. ***Приёмник***, в свою очередь, осуществляет ***демодуляцию*** сигнала, чтобы извлечь информацию из высокочастотного шумового компонента. Этот процесс схематично можно изобразить так, как показано на рисунке 4.

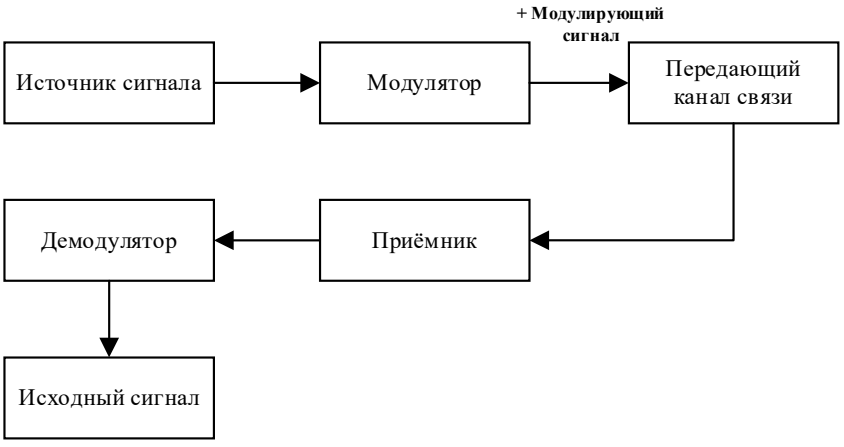

Рисунок 4 – Схемы для передачи и приема сигнала с помощью модуляции и демодуляции

Для реализации высокочастотного навязывания злоумышленник использует специальный ГВЧ (генератор высоких частот) и детектор, которые подключаются к телефонной линии, как показано на рисунке 5. Генератор высоких частот создает высокочастотный сигнал, который затем вводится на телефонную линию через передатчик. Детектор же подключается к телефонной линии для извлечения информации из измененного сигнала.

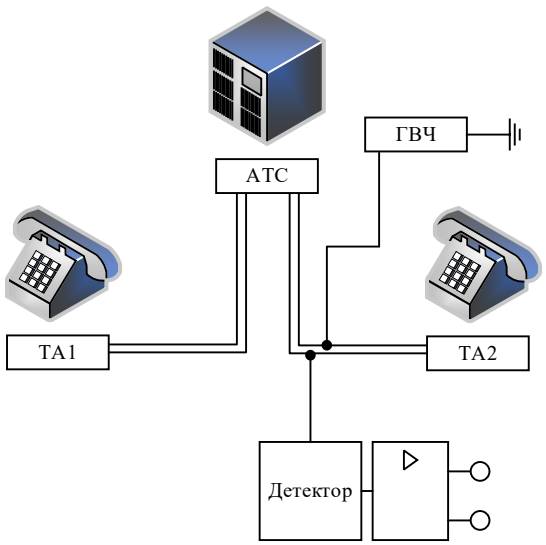

Рисунок 5 – Схема реализации метода ВЧ-навязывания

Злоумышленник может использовать высокочастотный сигнал для внесения помех в передаваемый сигнал, что позволяет ему записывать разговоры или получать доступ к конфиденциальной информации. Для применения данного метода злоумышленнику необходимо находиться в непосредственной близости от телефонной линии.

Корпус передатчика и детектора должен быть подключен к общей земле, чтобы обеспечить правильную работу электрических цепей. Это необходимо для того, чтобы генератор высоких частот и детектор могли функционировать правильно и избежать возможного повреждения электронных компонентов. Схема детектора приведена на рисунке 6.

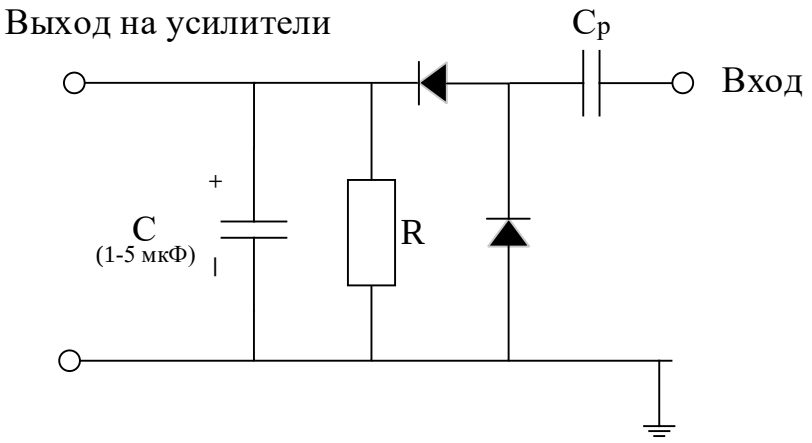

Рисунок 6 – Схема детектора, используемого при высокочастотном навязывании

Высокочастотное навязывание, как правило, использует сигналы с частотой f от 10 кГц до 1 МГц. Обусловлено это тем, что такой диапазон частот позволяет избежать шумов и помех, которые могут возникнуть в более высоких или низких диапазонах частот. При этом, используемые частоты могут варьироваться в зависимости от характеристик линии связи и требований злоумышленника. Тем не менее, если не используются специальные устройства для перехвата и анализа сигналов на линии без ее занятия, обнаружить навязывание несложно: при звонке по тому номеру, к каналу которого подключена аппаратура, занятость линии будет обнаружена.

2.3 Метод внедрения устройств в телефонный аппарат

Установка устройств внутрь телефонного аппарата – это один из методов физической утечки информации, который заключается в установке скрытых устройств непосредственно в телефонный аппарат. Одним из методов проведения телефонных атак на целевые объекты является внедрение устройства подслушивания (прослушки) в сам телефонный аппарат. Этот способ позволяет злоумышленнику слушать все телефонные разговоры, проходящие через аппарат, без необходимости подключения к линии связи [8].

Другим вариантом могут служить закладки с передачей акустической информации по телефонной линии, которые позволяют записывать разговоры и

передавать их по телефонной линии на удаленный телефон или записывающее устройство. В целом, в проводные телефонные аппараты могут быть внедрены самые разные устройства для съема информации, среди которых:

- ***Средства для записи разговоров***: это могут быть простые кассетные записывающие устройства или цифровые рекордеры;
- ***Аппаратные средства для перехвата сигнала***: устройства, которые позволяют не только прослушивать разговоры, но и записывать их в реальном времени;
- ***Вредоносное программное обеспечение***: в зависимости от сложности и функциональности ТА, злоумышленники могут внедрять в него вредоносные программы, которые позволяют им перехватывать телефонные разговоры и передавать их на удаленный сервер;
- ***Устройства для внедрения шумов на линию связи***: такие устройства создают шум на линии связи, что затрудняет прослушивание разговоров;
- ***Устройства для подмены номера***: такие устройства могут быть встроены в телефонный аппарат или подключены к нему через разъем для наушников и позволяют злоумышленникам подменять номер телефона, с которого происходит звонок.

Отдельно упомянем такое устройство, как ***транспондер*** (англ. «transponder» — «**trans**mitter-res**ponder**» — передатчик-ответчик) – электронное устройство, которое используется для передачи сигнала, полученного с одной линии связи, на другую линию связи. Очевидно, что его можно использовать для перехвата и передачи информации в проводных телефонных каналах [9]. Для работы транспондера его необходимо физически подключить к линии связи, как показано на рисунке 7.

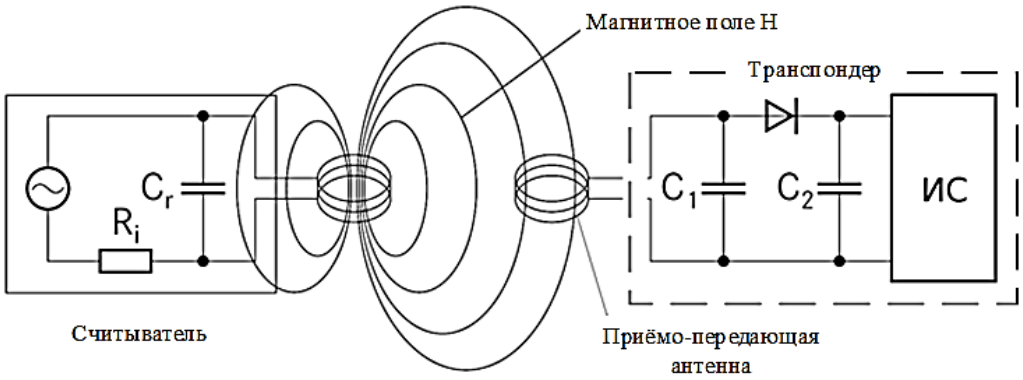

Рисунок 7 – Принципиальная схема транспондера

Поскольку транспондеры могут работать на частотах, необходимых для передачи телефонной связи, они могут обойти многие методы обнаружения утечки информации. Такие приёмники-передатчики применяются в современной и распространенной технологии RFID (англ. «Radio Frequency IDentification») – способ автоматической радиочастотной идентификации объекта. Принцип действия RFID технологии прост: посредством радиосигнала определенной частоты считываются и записываются данные, хранящиеся в транспондерах или, как их еще называют, RFID-метках или RFID-тегах.

2.4 Съём информации при подключении к телефонной линии

Подслушивание, сопровождаемое непосредственным подключением к телефонной линии, являются одним из наиболее распространенных методов съёма информации. Для проведения таких атак злоумышленникам необходимо иметь физический доступ к линии, который может быть получен путем вскрытия оборудования или через узел связи.

Можно выделить следующие методы подключения к телефонной линии:

1) Последовательное подключение

При последовательном подключении средства подслушивания с телефонным аппаратом и АТС, питание происходит за счет электрической энергии, которую передает телефонная линия. Использование трубки ремонтника является одним из способов осуществления последовательного

подключения средства подслушивания к телефонной линии. Такой способ получил широкое распространение в прошлом, когда телефонные линии были аналоговыми и подключение было более простым [4]. Схема такого подключения изображена на рисунке 8.

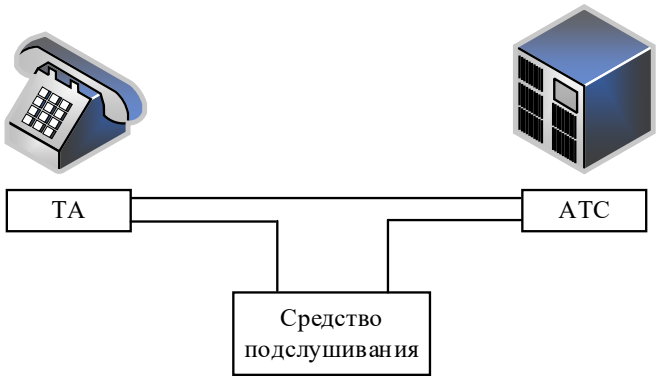

Рисунок 8 – Последовательное подключение к телефонной линии для съёма информации

Суть этого способа заключается в использовании специальной трубки, которая вставляется между телефонным аппаратом и кабелем, соединяющим его с линией связи. Трубка имеет внутри две контактные пружины, которые прижимаются к проводам кабеля, обеспечивая подключение. После подключения трубки, средство подслушивания может быть подключено к ней последовательно. Однако в настоящее время, когда телефонные линии стали цифровыми и технологичными, такой способ стал менее эффективным и редко используется.

2) Параллельное включение в линию связи

К линии связи подключается дополнительный провод, через который злоумышленник может получать доступ к разговорам. Такое подключение можно осуществить, например, в распределительных коробках, на местах соединения кабелей и т.п. При параллельном подключении устройства к линии связи сопротивление в цепи может измениться. Например, если устройство имеет высокое сопротивление, то при его подключении параллельно с телефоном общее сопротивление цепи увеличится, что может привести к

снижению качества связи. С другой стороны, если устройство имеет низкое сопротивление, то его подключение параллельно с телефоном может привести к снижению сопротивления цепи, что также может повлиять на качество связи [8]. Схематичное изображение такого подключения изображено на рисунке 9.

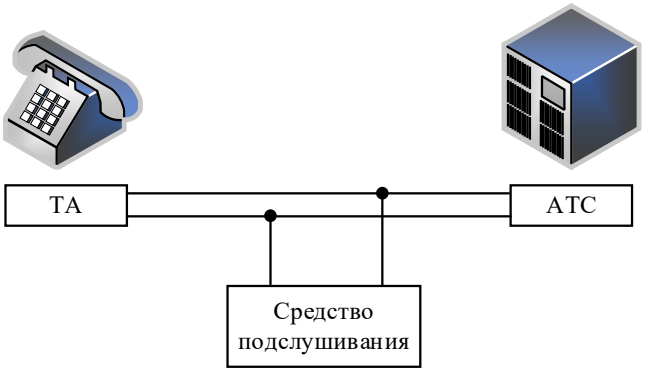

Рисунок 9 – Параллельное подключение к телефонной линии для съёма информации

3) Намотка проводка на линию связи

Подключение подслушивающего устройства с помощью намотки провода на линию связи основано на использования закона электромагнитной индукции (закон Фарадея), который формулируется следующим образом: *ЭДС индукции в замкнутом контуре равна и противоположна по знаку скорости изменения магнитного потока через поверхность, ограниченную контуром*. Его можно описать следующей аналитической формулой:

$$\varepsilon_i = -\frac{\Delta\varphi}{\Delta t}$$

Поскольку на линию связи наматывается провод, через который пропускается переменный ток с частотой, равной частоте сигнала на линии, можно считать, что контур состоит из N витков, то можно принять его за катушку индуктивности, а формулу можно преобразовать к виду:

$$\varepsilon_i = -N\frac{\Delta\varphi}{\Delta t}$$

При этом вокруг провода создается магнитное поле, которое может взаимодействовать с электромагнитным полем на линии связи и вызывать появление тока в намотке. Схематичное изображение такого подключения изображено на рисунке 10.

Рисунок 10 – Индуктивное подключение для съёма информации (с помощью намотки) на линию связи

Съём информации осуществляется с помощью приборов для анализа электромагнитных полей, например, специализированных индукционных зондов, которые могут обнаруживать и записывать электромагнитные поля, создаваемые передаваемым сигналом. Здесь с физической точки зрения важным аспектом является ***взаимоиндукция*** – явление возникновения ЭДС индукции в одном контуре при изменении силы тока во втором контуре и наоборот. Формула взаимной индукции описывает явление взаимного влияния электрических токов или переменных магнитных полей на индукцию электромагнитной силы в соседних проводах или катушках:

$$\varepsilon_1 = -M_{12}\frac{\Delta I_2}{\Delta t}$$

$$\varepsilon_2 = -M_{21}\frac{\Delta I_1}{\Delta t}$$

где $M_{12} = M_{21} = M$ – коэффициент пропорциональности (взаимной индукции), или иначе – взаимная индуктивность контуров.

4) Расположение провода вблизи линии связи

Этот метод основан на создании ёмкостного каскада между линией связи и прослушивающим устройством: при близком расположении провода средства подслушивания и самой линии между ними возникает ёмкость в результате наличия диэлектрика (например, воздуха) между двумя электрически заряженными телами. При таком подключении информация извлекается благодаря изменению электрического поля в окружении линии связи, вызванного наличием провода, расположенного рядом с ней. Ёмкость между проводом и линией создает переменное электрическое поле, которое возбуждает переменное электрическое поле в линии связи. Это приводит к появлению электрических сигналов в проводе, которые могут быть усилены и декодированы, чтобы получить информацию, передаваемую по линии связи. Схематичное изображение ёмкостного подключения изображено на рисунке 10.

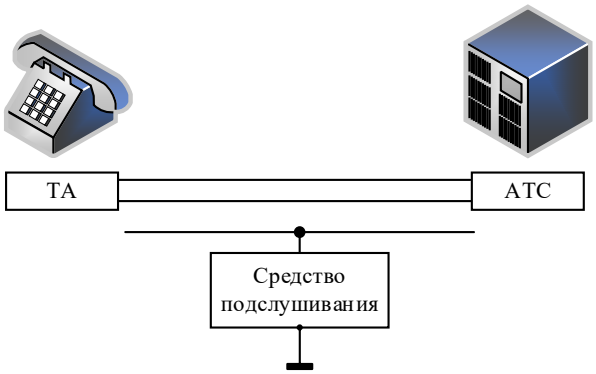

Рисунок 10 – Ёмкостное подключение для съёма информации вблизи линии связи

При последовательном и параллельном подключении средства подслушивания к линии связи, информация снимается непосредственно с провода, на котором установлено устройство. Обычно это происходит путем подключения к устройству осциллографа или другого прибора для анализа

сигналов. Данный прибор позволяет проанализировать сигнал на наличие шумов, фоновых шумов и других характеристик, связанных с передаваемой информацией.

III. Методы защиты информации, передаваемой по телефонному каналу

3.1 Методы обнаружения утечки информации в проводных телефонных каналах

Одним из самых эффективных способов защиты – это своевременный поиск уязвимостей и их анализ, который необходимо проводить заранее, ещё до начала воздействий со стороны злоумышленника, чтобы минимизировать ущерб. Это подтверждается на примере реальных случаев утечек информации, например, в 2018 году российские СМИ на портале РБК сообщили о том, что сотрудниками одной из крупных торговых сетей было обнаружено нелегальное подключение к проводной линии, которое позволяло злоумышленникам записывать все телефонные разговоры, происходившие в магазине. В результате были украдены данные более чем 150 тысяч банковских карт клиентов [7].

Современные технологии предоставляют злоумышленникам множество способов атак на телефонные каналы связи, поэтому необходимо постоянно обновлять методы защиты и следить за появлением новых угроз. Современные проводные телефоны претерпели значительные изменения: сейчас наиболее распространены телефоны с цифровым дисплеем, поддержкой многоканальной связи, встроенными микрофонами и динамиками, а в некоторых моделях есть возможность подключения к интернету. В связи с этим, для защиты проводных телефонов необходимо учитывать новые возможности, которые могут привести к утечке информации. Например, встроенные микрофоны и динамики могут использоваться злоумышленниками для прослушивания разговоров, а подключение телефонов к интернету также может привести к утечке информации, если не обеспечить защиту сетевого трафика.

Существует несколько методов обнаружения утечки информации в проводных телефонных каналах, каждый из которых имеет свои преимущества и недостатки. Наиболее часто используемые и эффективные методы включают в себя:

- использование специальных устройств для обнаружения и анализа электромагнитных сигналов на линии связи, таких как частотомеры, осциллографы, спектральные анализаторы, спектрометры и др.
- использование специализированных программных средств, которые могут автоматически обнаруживать и анализировать аномальные электромагнитные сигналы на линии связи.
- использование физических методов, таких как измерение электрического сопротивления и проведение тестов на короткое замыкание, для обнаружения наличия незаконного оборудования на линии связи.

Один из таких методов – это ***метод активной помехи***. Его суть заключается в том, что на линию связи подаются импульсы, которые создают помехи в канале и мешают передаче данных. При наличии средства подслушивания на линии связи помехи будут изменены, что позволит обнаружить утечку информации. Другим способом обнаружения утечек является ***метод анализа электромагнитного излучения***. Он заключается в том, что на кабель подаются электрические импульсы, а затем анализируется электромагнитное излучение, которое возникает в результате передачи сигнала по кабелю. Если на линии связи присутствует средство подслушивания, то электромагнитное излучение будет изменено, что позволит обнаружить его наличие [9].

Существуют также методы обнаружения утечки информации с помощью специальных устройств, называемых ***линейные трассеры*** (от англ. «line tracer», буквально – «отслеживатель линии»). Они используются для определения местонахождения утечки информации в проводных кабелях. Принцип их работы заключается в том, что на линию связи подаются специальные сигналы, которые затем прослеживаются с помощью линейного трассера. Этот метод может быть полезен при поиске средства подслушивания, которое было установлено в каком-то конкретном месте на линии связи.

Использование приборов для обнаружения аномальных изменений в электрических параметрах телефонной линии, а также установку дополнительных устройств защиты, таких как блокировщики передачи данных, также необходимо для защиты информации от съёма. Для ***измерения сопротивления*** проводника на телефонной линии можно использовать специализированный измеритель сопротивления или мультиметр. Этот прибор позволяет измерить сопротивление на линии и определить, есть ли аномальное изменение, указывающее на наличие злоумышленника. ***Анализатор спектра*** используется для анализа электрических сигналов на различных частотах. Он может помочь выявить аномальные изменения в спектре сигнала на телефонной линии, которые могут указывать на наличие внешних помех или несанкционированного подключения. ***Анализатор временных доменов*** позволяет изучать временную форму сигналов на линии. С его помощью можно обнаружить аномалии, такие как периодические импульсы или необычные шумы, которые могут свидетельствовать о вмешательстве злоумышленника. Для блокировки работы (например, набора номера) несанкционированно подключенных параллельных телефонных аппаратов используются специальные ***электронные блокираторы***. [8]

3.2 Физические методы защиты информации в проводных телефонных каналах

В соответствии с приведёнными ранее способами перехвата и съёма информации с использованием телефонных аппаратов и телефонных линий связи, рассмотрим далее методы защиты от указанных воздействий. Так, например, для обеспечения помехозащищенности информационных сигналов и защиты информации, обрабатываемой в технических средствах, от утечки по каналам побочных электромагнитных излучений и наводок, в частности рассмотренного ранее высокочастотного навязывания, как правило, используются ***помехоподавляющие LC-фильтры,*** а также экранировании

линий связи от внешних электромагнитных помех. Примеры схем фильтра верхних частот приведены на рисунке 11.

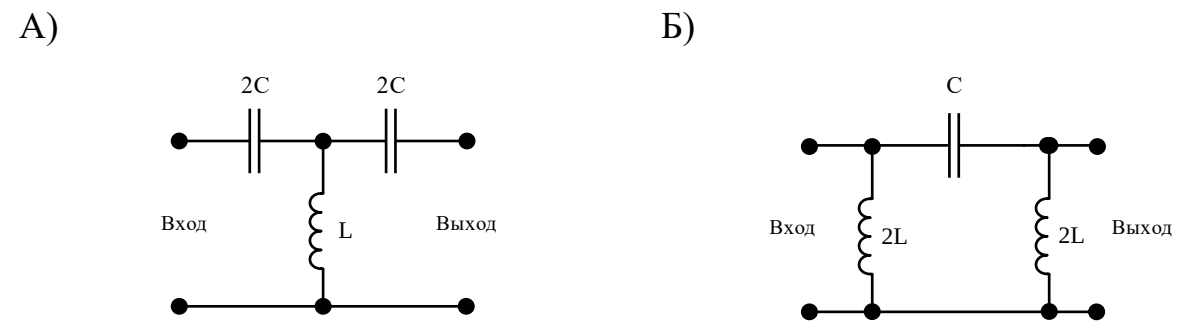

Рисунок 11 – Схемы ФВЧ: а) Т-образный; б) П-образный

Экранирование – применение экранных оболочек или металлических экранов вокруг проводников для предотвращения нежелательных излучений:

А) электростатическое излучение;

Б) магнитостатическое излучение;

В) электромагнитное излучение.

В настоящее время для создания сетей связи, как правило, используются кабели, жилы (проводники) которых попарно скручены между собой, вследствие чего они называются витой парой. Их экранирование может выглядеть следующим образом, как показано на рисунке 12.

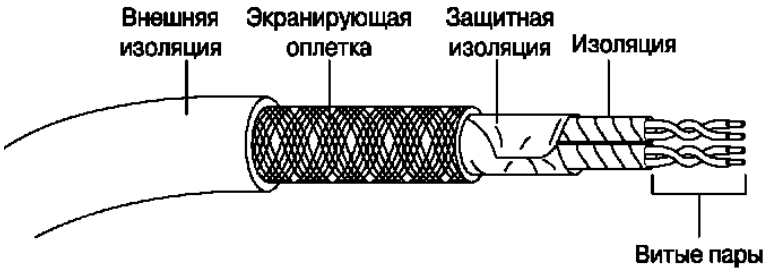

Рисунок 12 – Экранирование кабелей связи

На высоких частотах используются так называемые ***коаксиальные кабели***, состоящие из центрального проводника, который окружен изоляцией,

экранированным слоем и внешней оболочкой. Коаксиальный кабель получил свое название из-за того, что центральный проводник и внешний экран (оболочка) симметрично расположены вдоль одной оси – отсюда термин «коаксиальный» [10].

При ***электростатическом экранировании*** экранирующая оболочка создает проводящую поверхность, которая распределяет электростатический заряд по всей поверхности и снижает электрическое поле внутри области экранирования. ***Магнитостатическое экранирование*** основан на том, что металлическая оболочка или экран создает магнитный барьер, который препятствует распространению магнитных полей внутрь или изнутри экранированной области.

Электромагнитное экранирование используется для предотвращения электромагнитного излучения и помех. Металлическая экранирующая оболочка или экран блокирует прохождение электромагнитных волн и помех, создавая физическую преграду для их распространения. Такое экранирование помогает предотвратить воздействие внешних электромагнитных полей на проводники и электронные компоненты внутри экранированной области, а также предотвратить утечку собственных электромагнитных излучений, которые могут нежелательно влиять на другие системы и устройства.

Для обнаружения и защиты от прослушивания применяются ***телефонные линейные тестеры***, которые помогают обнаружить аномалии наподобие снижения сопротивления или наличия дополнительных сигналов, которые могут указывать на подключение прослушивающих устройств. Целесообразно позаботиться и о защите помещений, где могут проводиться конфиденциальные телефонные переговоры. Так, для создания фонового шума или помех, которые затрудняют или делают сложным прослушивание конфиденциальных разговоров или передачу данных используют ***генераторы случайного шума***. Упомянутое ранее экранирование может быть применено не только к непосредственно линиям связи, но и к самим помещениям: применение

материалов с высокой экранирующей способностью, таких как металлические оболочки, для создания защищенных помещений, недоступных для электромагнитного излучения.

Ещё одним аспектом, которым может помочь при защите информации от утечки по телефонным каналам может стать использование оптоволоконных кабелей вместо медных, так как оптоволокно передает информацию в виде световых импульсов, а не электрических сигналов. Такие кабели более сложны в использовании для съема информации, так как они не излучают электромагнитное поле. Стоит отметить, что мероприятие по замене медных кабелей на оптоволоконные является дорогостоящим, однако снизить затраты можно использование волоконно-оптических усилителей, которые позволяют передавать сигналы на большие расстояния без потери качества. Это может существенно снизить количество необходимых оптоволоконных кабелей и, соответственно, снизить затраты на установку и эксплуатацию такой системы связи [2]. Также можно использовать более дешевые типы оптоволоконных кабелей, такие как многомодовые кабели, вместо более дорогих одномодовых кабелей. Однако следует понимать, что использование менее качественных кабелей может снизить эффективность защиты от утечки информации.

Анализируя многообразие рассмотренных методов защиты, можно заключить, что их выбор должен опираться на потребности конкретной системы. С помощью приведённых методов можно обеспечить достаточный уровень защиты для сохранения конфиденциальности информации, передаваемой по проводным телефонным каналам связи, при условии, что используемые устройства защиты будут своевременно совершенствоваться в соответствии с актуальными особенностями угроз и методов воздействия на систему.

Заключение

Телефонные каналы по-прежнему остаются одним из самых распространенных средств связи. В связи с быстро развивающимися технологиями и новыми методами атак на телефонные каналы, защита этих каналов становится все более сложной задачей – необходимо понимать особенности их работы с физической и технологической точек зрения, чтобы анализировать уязвимости и предотвращать возможные утечки. Защитники информации должны постоянно совершенствовать свои методы защиты, чтобы оставаться впереди злоумышленников. В свою очередь, злоумышленники также ищут новые способы для преодоления защиты и получения доступа к ценной информации.

Нельзя не признать, что между защитниками информации и злоумышленниками существует настоящая технологическая гонка, преуспеть в которой можно лишь благодаря постоянному совершенствованию технологий защиты и развитию новых методов анализа и обнаружения атак.

В ходе выполнения данной курсовой работы были рассмотрены основные аспекты работы проводных телефонов и телефонных каналов связи, их физические особенности функционирования, а также приведены методы защиты от возможной утечки информации в соответствии с описанными уязвимостями телефонных аппаратов и сетей их связи.

Список использованных источников

1. Хорев А.А. Защита информации от утечки по техническим каналам. Часть 1. Технические каналы утечки информации. Учебное пособие. М.: Гостехкомиссия России, 1998. - 320 с.
2. Евсеев А. Н. Радиолюбительские устройства телефонной связи. — М.: Радио и связь, Малип, 1999. — 112 с; ил. — (Массовая радиобиблиотека; Вып. 1225).
3. Кузнецов А.А., Брызгалов Д.В., Макарова Е.С. "Определение параметров линий связи по измерениям их собственных электрических параметров". Электроника: научно-технический журнал. 2016. № 7. С. 38-43.
4. Кутуев Р.Ф., Кутуева Ф.Р. Безопасность сетей связи. Санкт-Петербург: Питер, 2016.
5. Ляхов А. Методы и средства защиты информации. Москва: Изд-во МГТУ им. Н.Э. Баумана, 2015.
6. Verizon's 2020 Data Breach Investigations Report // Verizon URL: https://www.verizon.com/ (дата обращения: 07.05.2023).
7. В магазинах крупной торговой сети нашли нелегальные записи телефонных разговоров // РБК URL: https://www.rbc.ru/technology_and_media/12/03/2018/ (дата обращения: 07.05.2023).
8. Специальная техника: каталог / НПО "Защита информации". - М. : НПО "Защита информации", 1998. - 32 с.
9. Технические средства и методы защиты информации: Учебник для вузов / Зайцев А.П., Шелупанов А.А., Мещеряков Р.В. и др.; под ред. А.П. Зайцева и А.А. Шелупанова. – М.: ООО «Издательство Машиностроение», 2009 – 508 с.
10. Портнов, Э. Л. Принципы построения первичных сетей и оптические кабельные линии связи : учебное пособие / Э. Л. Портнов. — Москва : Горячая линия-Телеком, 2017. — 544 с. — ISBN 978-5-9912-0071-4. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/111090 (дата обращения: 14.05.2023)

Приложение

Таблица 1 – Основные электрические параметры телефонного аппарата (ГОСТ 7153-85)

Название параметра	**Норма по классам сложности**			
	0	1	2	3
Максимально допустимое напряжение собственного шума, мВ	0,5	0,5	0,5	0,4
Модуль входного электрического сопротивления:				
а) разговорный режим, Ом	450-800	450-800	-	-
б) минимум при ожидании вызова, Ом	10^4	10^4	-	-
в) минимум в режиме вызова, Ом	$4*10^3$	$4*10^3$	-	-
Электрическое сопротивление постоянному току (Ом) в разговорном режиме при токе $i = 35$ *мА*:				
а) в вертикальном положении трубки	160-400	160-400	180-400	≤ 320
б) в горизонтальном положении трубки	160-400	160-400	160-400	≤ 600
Электрическое сопротивление постоянному току (Ом) в режиме набора номера для т/а с импульсным способом передачи при токе $i = 35$ *мА*:				
а) максимум при замыкании шлейфа, Ом	160	150	50	-
Максимум постоянного тока, потребляемый в режимах ожидания вызова и отбоя, мА	8	8	8	8
Время разрыва шлейфа для т\а с устройством нормированного разрыва шлейфа	80 ± 40	80 ± 40	-	-
Минимальная значимость программируемого набора номера	8	8	8	-

Таблица 2 – Характеристики основных сигналов, поступающих от АТС к АУ (ГОСТ 7153-85)

Название сигнала	**Длительность, с**		**Уровень, дБ или напряжение, В**	**Частота, Гц**
	Импульс	**Пауза**		
Ответ станции	Непрерывная передача		От -5 дБ до -30 дБ	425 ± 25
Посылка вызова	0,8 + 0,1 или 1 + 0,1	3,2 + 0,1 или 4 + 0,1	От 16 В до 110 В	16…50

Таблица 2 – Характеристики основных сигналов, поступающих от АТС к АУ (продолжение)

Название сигнала	**Длительность, с**		**Уровень, дБ или напряжение, В**	**Частота, Гц**
	Импульс	**Пауза**		
Контроль посылки вызова	0,8 ± 0,1 или 1 ± 0,1	3,2 ± 0,1 или 4 ± 0,1	От -5 дБ до +30 дБ	425 ± 25
Занято	От 0,3 до 0,4	От 0,3 до 0,4	От -5 дБ до -30 дБ	425 ± 25
Занято-перегрузка	От 0,16 до 0,2	От 0,16 до 0,2	От -5 дБ до -30 дБ	425 ± 25
Указательный (частоты чередуются в указанном порядке)	0,33 ± 0,07 0,33 ± 0,07 0,33 ± 0,07	0,33 ± 0,003 0,33 ± 0,003 1 ± 0,25	От -5 дБ до -30 дБ От -5 дБ до -30 дБ От -5 дБ до -30 дБ	950 ± 50 1400 ± 50 1800 ± 50
Предупреждение	0,4 ± 0,04	15 ± 3	От -10 дБ до -35 дБ	425 ± 25
Вмешательство (паузы чередуются в указанном порядке)	0,25 ± 0,025	0,25 ± 0,025 1,25 ± 0,3	От -10 дБ до -35 дБ	425 ± 25
Уведомление	0,25 ± 0,025	5,525 ± 0,8	От -10 дБ до -35 дБ	1400 ± 20
Предупреждение об окончании оплаченного интервала времени	0,4 ± 0,04	5,525 ± 0,8	От -10 дБ до -35 дБ	1400 ± 20
Неполный состав участников или отключение участника	От 0,3 до 1	Одиночный импульс	От -10 дБ до -35 дБ	425 ± 25