ГОСУДАРСТВЕННЫЙ КОМИТЕТ СВЯЗИ, ИНФОРМАТИЗАЦИИ И ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ РЕСПУБЛИКИ УЗБЕКИСТАН

НУКУССКИЙ ФИЛИАЛ ТАШКЕНТСКОГО УНИВЕРСИТЕТА ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

ФАКУЛЬТЕТ «КОМПЬЮТЕРНЫЙ ИНЖИНИРИНГ»

КАФЕДРА «ТЕЛЕКОММУНИКАЦИОННЫЙ ИНЖИНИРИНГ»

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА

на тему «**Защита абонентских линии от несанкционированного доступа**»

Выполнил: выпускник 4-курса по направлению «Телекоммуникация»
студент
Кожаметова Ж._____

НАУЧНЫЙ РУКОВОДИТЕЛЬ:
Специалист филиала
гражданской защиты
Рес.КК. АК «Узбектелеком»
Садикова З. _____

Выпускная квалификационная работа прошла предварительную защиту на кафедре
Протокол № _____ от «___» _____ 2014 г.

НУКУС - 2014 г.

ГОСУДАРСТВЕННЫЙ КОМИТЕТ СВЯЗИ, ИНФОРМАТИЗАЦИИ И ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ РЕСПУБЛИКИ УЗБЕКИСТАН
НУКУССКИЙ ФИЛИАЛ ТАШКЕНТСКОГО УНИВЕРСИТЕТА ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

ФАКУЛЬТЕТ «КОМПЬЮТЕРНЫЙ ИНЖИНИРИНГ»
КАФЕДРА «ТЕЛЕКОММУНИКАЦИОННЫЙ ИНЖИНИРИНГ»

У Т В Е Р Ж Д А Ю
Зав. кафедрой _____
«____» _____ 201_ г.

ЗАДАНИЕ

на выпускную квалификационную работу Кожаметова Жамила Полатбаевна
(фамилия, имя, отчество)

1.Тема работы: Защита абонентских линии от несанкционированного доступа»
2.Тема утверждена приказом НФ ТУИТ от «04» 03 2014 г.№122
3. Срок сдачи законченной работы «02» 06 2014 г.
4. .Исходные данные к работе: номенклатура цифровых автоматических телефонных станций (ЦАТС) зарубежного производства, средства защиты информации в абонентских линиях
5.Содержание расчетно-пояснительной записки (перечень подлежащих разработке вопросов): Введение. Основные проблемы защиты информации в абонентских линиях телефонной сети общего пользования, Общие принципы и методы защиты информации в абонентских линиях ТфОП, заключение, литература.
6.Перечень графического материала: постановка задачи, Анализ абонентских линий сетей телекоммуникаций как объекта защиты от несанкционированного доступа к услугам телекоммуникаций, методы защиты от несанкционированного доступа к услугам телекоммуникаций.
7. Дата выдачи задания 23.03.14г.

Руководитель _____
(подпись)

Задание принял _____
(подпись)

Консультанты по отдельным разделам выпускной работы

Раздел	Ф.И.О. руководителя	Подпись, дата	
		Задание выдал	Задание получил
Основная часть	Садикова Замира	23.03.14	23.03.14
Безопасность жизнедеятельности	Садикова Замира	23.03.14	23.03.14

График выполнения работы

№	Наименование раздела работы	Срок выполнения	Отметка руководителя выполнении
1.	Основные проблемы защиты информации в абонентских линиях телефонной сети общего пользования	15.01.14 - 15.03.14	
2.	Общие принципы и методы защиты информации в абонентских линиях ТфОП	16.03.14-10.05.14	
3.	Безопасность жизнедеятельности	11.05.14-15.05.14	
4.	Заключение	17.05.14-31.05.14	

Выпускник _____ «____» _____2014 г.
(подпись)
Руководитель_____ «____» _____2014 г.
(подпись)

В данном ВКР рассмотрены общие принципы защиты информации в абонентских линиях, организационные и технические меры защиты информации, показаны особенности защиты информации в абонентских линиях, проведен анализ различных подходов к защите информации в абонентских линиях и рассмотрены средства защиты.

Ушбу малакавий ишида абонент тармоқларида ахборотларни химоя қилишнинг умумий тамоиллари, ахборотларни химоя қилишнинг ташкиллаштирувчи ва техник чоралари, абонент тармоқларида ахборатларни химоя қилишнинг хусусиятлари, абонент тармоқларида ахборотларни химоя қилиш қуроллари ва ҳар ҳил методларининг анализи келтирилган.

In this final qualifying work general principles of the protection of information in subscriber lines, organizational and technical measures to protect information, information protection features shown in subscriber lines, the analysis of different approaches to data protection in subscriber lines and discussed remedies.

Содержание

ВВЕДЕНИЕ

Между народный опыт развитых стран показывает, что развитая инфокоммуникационная инфраструктура оказывает все большее влияние на развитие экономики, бизнеса и других сфер деятельности, общества. Одновременно решению проблем обеспечения информационной безопасности инфокоммуникационной инфраструктуры уделяется все большее внимание, поскольку в современных условиях информационная безопасность становится важнейшей составляющей национальной безопасности любого государства. Высшие органы государственной власти этих стран уделяют все большее внимание созданию и развитию информационно-телекоммуникационных технологий с одновременным, обеспечением их информационной безопасности.

Основные проблемы современного этапа развития сферы связи и информатизации связаны с существенным ростом сложности и наукоемкости инфокоммуникационных технологий, так как технические и программные средства потенциально содержат в себе большое число ошибок и недекларируемых возможностей, которые могут быть использованы злоумышленниками.

В настоящее время на сетях телекоммуникаций Республики Узбекистан используется широкая номенклатура цифровых автоматических телефонных станций (ЦАТС) зарубежного производства. Как показывает международная практика, применение технологически небезопасных технических средств и программного обеспечения, а также возможность его модификации, могут привести к несанкционированному доступу (НСД) к информации вплоть до блокировки ЦАТС. В этой связи естественно возникают следующие вопросы:

- какие существуют пути НСД к информации в зарубежных ЦАТС;
- как обеспечить защиту информации при использовании ЦАТС;
- как убедиться в том, что применяемые средства защиты в ЦАТС обеспечивают требуемый уровень безопасности информации.

Многочисленными исследованиями установлено, что в защите ЦАТС выделяются следующие направления:

- закрытие технических каналов утечки информации;

- закрытие каналов передачи информации;

- обеспечение защиты от НСД к информации в абонентских и соединительных линиях, в коммутационной и управляющих подсистемах ЦАТС, включая программное обеспечение (ПО);

- использование ПО, проверенного на отсутствие возможностей, не декларированных в технической документации.

Одним из важных направлений решения этой проблемы является сертификация ЦАТС по требованиям безопасности информации. В свою очередь решение проблемы сертификации ЦАТС по требованиям безопасности информации должно основываться на положениях и требованиях законов, стандартов и нормативно-методических документов по защите информации от НСД. Международный опыт показывает, что сертификационные испытания ЦАТС по требованиям безопасности информации являются сложным и наукоемким процессом, это связанно с тем, что разработка нормативных, руководящих и методических документов, касающихся сертификационных испытаний по требованиям информационной безопасности, требует проведения глубоких научных исследований и постоянного научно-методического и технического сопровождения.

Таким образом, в связи с широким использованием на сетях телекоммуникаций Республики Узбекистан разнообразных зарубежных цифровых коммутационных систем (включая ЦАТС) и автоматизированных систем управления сетями телекоммуникаций с соответствующим, программным обеспечением, у нарушителей появляются возможности воздействовать на сеть телекоммуникаций, не разрушая какие-либо её элементы физически, то есть воздействие носит неявный и обезличенный

характер. Исследования показывают, что наиболее подверженными воздействиям нарушителей являются абонентские линии (АЛ), поэтому в последнее время особую актуальность приобрела проблема защиты АЛ от НСД и решению этой проблемы посвящается большое количество практических работ.

Цель выпускной квалификационной работы: рассмотрение общих принципов защиты информации в абонентских линиях, организационные и технические меры защиты информации, показать особенности защиты информации в абонентских линиях и анализ различных подходов к защите информации в абонентских линиях и средства защиты.

Составные части выпускной квалификационной работы: ВКР состоит из введения, 3-х глав, заключения и из списка использованных литератур.

В первой главе рассмотрены основные принципы и способы доступа к абонентским линиям, типы нарушителей и мероприятия по защите информации от НСД...19.

Вторая глава посвящена анализе общих подходов к защите информации в абонентских линиях, принципы и методы защиты информации в абонентских линиях, средства защиты информации в абонентских линиях. Исследованы и доказаны, основные причины успешной реализации НСД к услугам. Исследованы решения задач, связанных с защитой АЛ от НСД.

В третьей главе рассмотрены мероприятия по безопасность жизнедеятельности.

1.ОСНОВНЫЕ ПРОБЛЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ В АБОНЕНТСКИХ ЛИНИЯХ ТЕЛЕФОННОЙ СЕТИ ОБЩЕГО ПОЛЬЗОВАНИЯ

1.1. Основные принципы и способы доступа к абонентским линиям

Как показывает международный опыт развитых стран, решение проблем информационной безопасности (ИБ) и защиты информации (ЗИ) должно основываться на положениях и требованиях соответствующих законов, стандартов и нормативно-методических документов. Известно, что гарантом обеспечения ИБ и ЗИ выступает государство, так как это право закреплено в конституции страны. С этой целью создается государственная система обеспечения ИБ и ЗИ и определяются головные организации по разработке руководящих документов в области ИБ и ЗИ.

Неукоснительное выполнение требований законодательства и своевременная разработка и принятие необходимых нормативно-правовых документов в области ИБ и ЗИ является мощной законодательно-правовой мерой предотвращения нарушений информационной безопасности, поэтому среди различных аспектов обеспечения ИБ и ЗИ, на сегодняшний день наиболее важными и актуальными являются вопросы нормативно-правового обеспечения.

В последние годы в Республике Узбекистан уделяется серьезное внимание созданию законодательной и нормативно-правовой базы в области ИБ и ЗИ в соответствии с международными требованиями.

В соответствии с законодательством Республики Узбекистан для телекоммуникационных компаний, предоставляющих услуги связи, является актуальной необходимость обеспечения защиты:

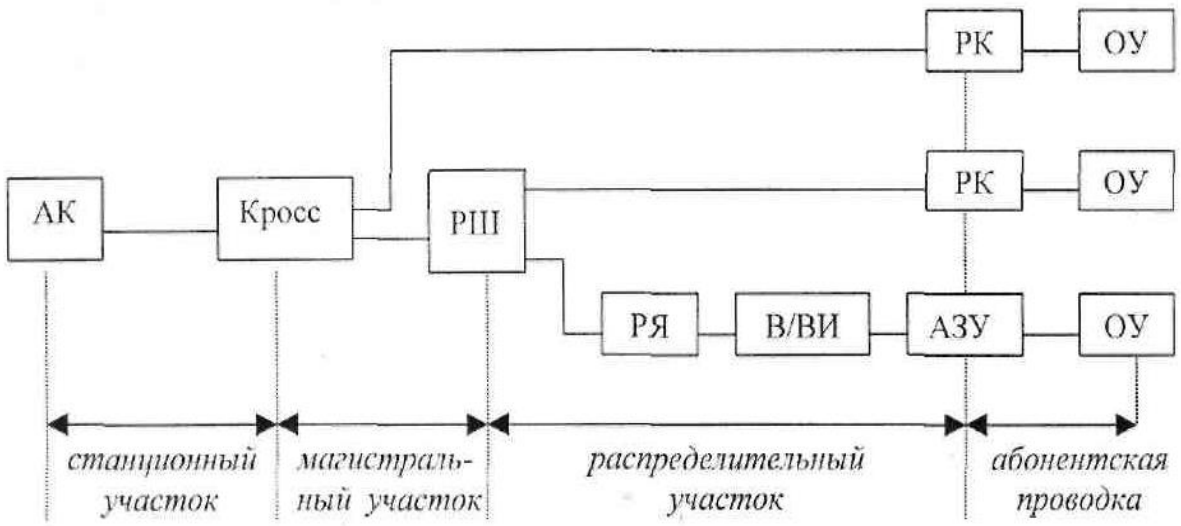
- тайны телефонных переговоров и иных сообщений;
- служебной и коммерческой тайны;
- персональных данных абонентов и др.

Однако используемые на телефонной сети общего пользования (ТфОП)

линейные сооружения, абонентские и соединительные линии, телефонные распределительные устройства в основе своей, остаются незащищенными от несанкционированного доступа (НСД). Это во многом связано с тем, что во время их строительства считалось, что угрозы безопасности не представляют особой проблемы и при проектировании ТфОП **в ее** составе не предусматривалось наличие специальных технических и физических средств защиты, которые позволяли бы оперативно выявлять факты НСД. Так как основным местом несанкционированных подключений является абонентская линия (АЛ), то и большинство угроз НСД связано с использованием недостатков **в** защите АЛ. В настоящее время отсутствие специальных средств защиты и недостаточный контроль за состоянием отдельных компонентов АЛ позволяет нарушителям осуществлять свою противоправную деятельность.

Как отмечалось ранее, одной из наиболее актуальных проблем является НСД к телефонной сети общего пользования, особенно это касается операторов, предоставляющих услуги междугородней и международной связи. Однако, в связи с переходом к повременной оплате телефонных разговоров эта проблема возникает и у операторов, предоставляющих услуги местной связи. К наиболее распространенным разновидностям НСД относится непосредственное физическое несанкционированное подключение (НСП) к абонентским линиям.

Как известно, наиболее уязвимыми являются те места абонентских линий (АЛ), где имеется возможность установления непосредственного несанкционированного физического подключения (контакта) с помощью простых средств. Обобщенная структурная схема абонентской линии предоставлена на рисунке 1.1 [1,2].



АК - абонентский комплект;

АЗУ - абонентское защитное устройство;

В/ВИ - вводно-выводные изоляторы;

ОУ - оконечное устройство;

РК - распределительная коробка;

РШ - распределительный шкаф;

РЯ - распределительный ящик.

Рисунок 1.1 - Структурная схема абонентской линии

К наиболее распространенным участкам несанкционированного подключения к АЛ относится промежуточное оборудование, которое имеет внешние контакты (клеммы), позволяющие без особого труда подключиться к линии, а также абонентская проводка, расположенная в легкодоступном месте. Для подключения на промежуточном оборудовании не требуется каких-либо дополнительных специальных средств.

Как показывает практика, используемое в реальных АЛ традиционное оконечное кабельное и распределительное оборудование практически не претерпело никаких изменений в направлении усиления его физической защиты, поэтому одним из главных факторов, приводящих к НСП к АЛ является то обстоятельство, что это оборудование не соответствует современным требованиям безопасности. К наиболее уязвимому с точки

зрения НСП к АЛ распределительному оборудованию вследствие его слабой защищенности и отсутствия контроля за его состоянием относятся:

- распределительные кабельные шкафы (РКШ);
- распределительные коробки (РК) и распределительные ящики (РЯ);
- абонентская проводка.

Повышение степени защиты АЛ от НСД предполагает переход на новую более высокую ступень организации ее безопасности и необходимость постоянного совершенствования защиты ее типовых компонентов (РКШ, РК, РЯ и др.).

Для обеспечения эффективной защиты АЛ от НСД необходимо:

- изучить возможные способы несанкционированных подключений к АЛ;
- представить неформальную модель потенциального нарушителя;
- на основе системного подхода использовать разнообразные мероприятия, методы и средства защиты информации в АЛ.

Как показывает международная практика, комплексный подход к организации защиты информации в АЛ представляет собой совокупность [3-9]:

- законодательно-правовых мер;
- морально-этических норм;
- организационных мероприятий;
- физических средств;
- технических (аппаратно-программных) средств. Только при комплексном использовании всех вышеуказанных мероприятий, мер, методов и средств может быть обеспеченно создание упреждающей (превентивной) стратегии защиты информации.

В этой связи актуальной задачей является разработка и реализация современной концепции защиты абонентских линий телефонной сети

общего пользования, которые являются наиболее уязвимой с точки зрения защиты информации частью телефонной сети общего пользования.

Как известно, все виды НСП к АЛ по длительности несанкционированного использования телефонного канала можно разделить на подключения кратковременные и длительные [2].

Кратковременное подключение характеризуется малым временем контакта несанкционированного терминального (оконечного) устройства с АЛ в точке подключения. Как правило, кратковременные подключения не требуют от злоумышленника тщательной маскировки мест подключения. Учитывая нынешнее состояние телефонной сети общего пользования, этот вид нарушения достаточно сложно обнаружить сразу, так как он очень часто имеет эпизодический характер, а выявляется абонентом лишь тогда, когда приходит счет на оплату междугородных или международных разговоров.

Длительное подключение характеризуется длительным временем контакта несанкционированного терминального устройства в точке подключения и частым использованием линии для незаконных переговоров. Для НСП используются либо обычные телефонные аппараты (ТА), либо специальные устройства подключения, обеспечивающие скрытое подсоединение к двухпроводному шлейфу и имитацию всех основных сигналов АТС для абонента.

Выявить подключение таких приборов без специального оборудования достаточно сложно. Обнаружение НСП очень часто происходит лишь после того, как абоненту приходят счета на оплату разговоров.

НСП по характеру места доступа к АЛ делятся на внутренние и внешние подключения.

Внутреннее подключение означает не подключение к АЛ как таковое, а использование нужного оконечного устройства в собственных корыстных целях.

Внешние подключения характеризуются непосредственным

подключением к АЛ и по способу подключения бывают контактными и бесконтактными.

Бесконтактные подключения осуществляются на абонентском участке, когда в качестве терминального устройства используется радиотелефон.

Контактные подключения по способам НСП к АЛ делятся на подключения с разрывом и без разрыва шлейфа.

Классификация способов НСП к АЛ приведена на рисунке 1.2.

Несанкционированное подключение без разрыва шлейфа производится параллельным подключением в РК, РЯ или РШ, к абонентской проводке и на других участках, где есть доступ к АЛ. Для этого способа подключения характерно прослушивание на ТА абонента набора номера, что позволяет абоненту вовремя обнаружить факт НСП к АЛ. Это подсоединение к двухпроводному шлейфу чаще всего производится обычным ТА с помощью разъёмов типа "крокодил" либо иголками, после чего практически невозможно обнаружить следы подключения.

Несанкционированное подключение с разрывом шлейфа характеризуется высокой степенью скрытности проведения нелегальных разговоров и практической невозможностью выявление факта подключения в момент его осуществления. Местом несанкционированного подключения может быть любой участок АЛ, но обычно им является РК, РЯ, РШ или абонентская проводка, причем после проведения разговора место тщательно маскируется, создавая дополнительные сложности для выявления факта НСП. Таким образом, основные методы несанкционированного доступа к цифровым АТС различаются, прежде всего, по цели [6, 7]:

- получение доступа с целью совершения платных вызовов за чужой счет;

Рисунок 2 - Классификация способов несанкционированного подключения к АЛ

- получение доступа с целью получения конфиденциальной информации, т. е. с целью прослушивания абонентов;
- получение доступа с целью нарушения телефонной связи;
- получение доступа с целью незаконного получения телефонного сервиса.

Получение несанкционированного доступа с целью совершения платных вызовов за чужой счет является самым распространенным в мире. Методы организации вызовов за чужой счет (рисунок 1.3) различаются по типу доступа на физические и логический. Физические методы, в свою очередь, бывают двух типов: несанкционированного подключения и подмены номера.

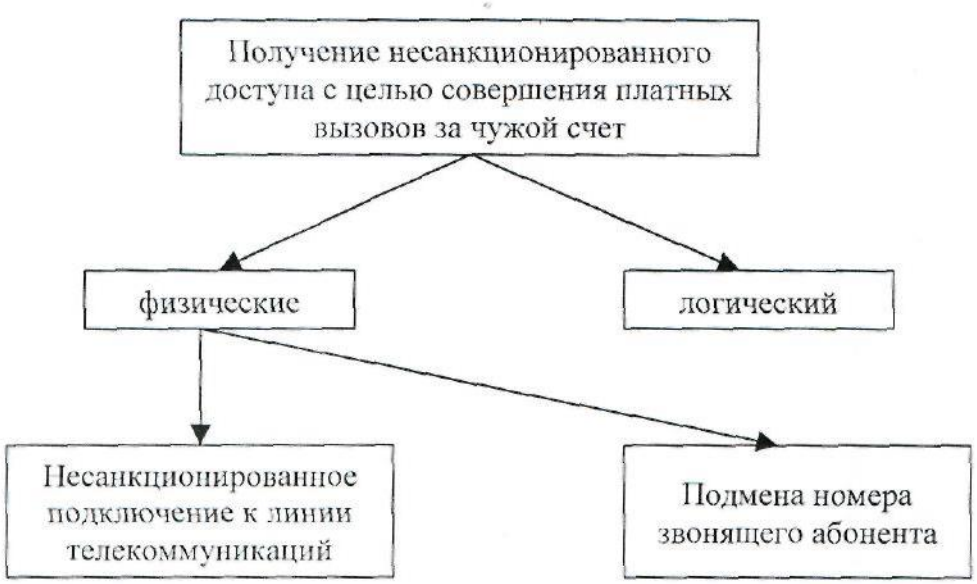


Рисунок 3 - Методы организации вызовов за чужой счет

Несанкционированное подключение к существующему номеру можно осуществить на АТС любого типа. Возможность такого подключения вообще обусловлена не свойствами АТС, а свойствами кабельного хозяйства. Любой компетентный человек, обладающий соответствующей аппаратурой (в отдельных случаях используется обыкновенный аналоговый телефон), может подключиться к АЛ и совершить платный вызов, за который придется платить владельцу или арендатору этой АЛ. Методы борьбы с такими типами несанкционированного доступа традиционны: ограничение доступа к кабельному хозяйству, установка аппаратуры, определяющей наличие/отсутствие параллельного подключения к АЛ, получение и анализ отчетов АТС о совершенных вызовах (получение тарификационных данных). К особенностям цифровых АТС (ЦАТС) относится возможность реализации следующих функций [6]:

-. введение уникального пароля для каждого пользователя при совершении платных вызовов. При наборе платного номера станция специальным сигналом запросит уникальный пароль (авторизационный код). Этот код можно выдать в тарификационных данных для определения автора платного вызова;

- организация перенаправления вызовов определенных номеров городской телефонной сети на любой номер как внутри телефонной станции, так и вне ее, например, на номер начальника службы безопасности. В этом случае злоумышленник, набравший запрещенный номер, дозвонится вместо набранного номера к сотруднику безопасности;

- введение уникального пароля для каждого телефонного аппарата в системе. При приходе на работу сотрудник вводит свой уникальный пароль, и его аппарат включается. Если сотрудник на время оставляет рабочее место, он вводит пароль, и аппарат выключается;

- фиксация номера и времени отключения какого-либо абонента от своей линии (некоторые ЦАТС имеют такую возможность), таким образом,

анализируя эту информацию, можно следить за несанкционированными подключениями к своим внутренним линиям.

Подмена номера на городских АТС производится следующим образом: при запросе автоматического определителя номера (АОН) в канал подключается аппаратура генерации АОНа. В этот момент злоумышленник дает в линию импульс высокой мощности, который выводит из строя эту аппаратуру и на повторный запрос дает уже измененный номер. Борьбу с этим видом телефонного воровства можно вести несколькими способами:

- установкой ЦАТС на городских телефонных сетях. ЦАТС лишены этого недостатка, так как принципы их функционирования несколько другие;
- ведением тотальной посекундной тарификации. Обладая этими данными, можно вычислить инициатора любого платного вызова, независимо от определенного номера. Однако, учитывая объем городского трафика, это чрезвычайно трудоемкая операция.

Подмену номера можно организовать также средствами учрежденческой АТС (УАТС). В случае, если УАТС подключается к городской АТС по соединительным линиям, эта УАТС обязана иметь возможность генерации собственного АОНа. Таким образом, существует вероятность того, что некий злоумышленник может использовать некую УАТС для осуществления такого рода мошенничества. Однако, подобные ситуации крайне редки и могут иметь разве что случайный характер, так как, во-первых, действуют вышеописанные средства борьбы, а во-вторых, степень окупаемости такого мошенничества слишком мала.

Каждая ЦАТС имеет специальный модуль удаленного получения ресурсов телефонной станции. У большинства ЦАТС этот модуль имеет название DISA (Direct Inward Station Access). DISA обеспечивает доступ к ресурсам ЦАТС извне, именно на этих модулях организуется функция «тонового донабора». Она дает возможность при вызове определенного

городского номера запросить дополнительный ввод в DTMF-режиме (тоновый режим, его поддерживает большинство телефонных аппаратов импортного производства). Это позволяет дать персональный телефонный номер каждому абоненту УАТС при условии наличия только одного городского телефонного номера. Однако этот модуль имеет множество функций: например, с его помощью можно осуществить любой, в том числе и платный, вызов за счет компании, где установлена эта цифровая УАТС. Такая возможность бывает очень полезна, поскольку:

1. Дешевле осуществить междугородный вызов с сотового телефона через УАТС;

2. Можно осуществить междугородный вызов по работе в дальние регионы (разница во времени более б.часов) из дома за счет компании;

3. Можно осуществить вызов абонента, которому не хотелось бы демонстрировать свой АОН, с сотового телефона, организовав "петлю вызова" через компанию;

4. Можно осуществить городской и междугородный вызов для проверки работоспособности телекоммуникационного оборудования;

5. Можно осуществить вызов в другой город по ведомственной телефонной сети.

Возможностей у этого модуля множество, однако, естественно, его использование создает в системе безопасности компании огромную "дыру". С его помощью злоумышленники могут осуществить любой платный вызов за счет компании, а в АТС некоторых типов - осуществить удаленное прослушивание любого абонента АТС, нарушить нормальную работу АТС и т.д. Поэтому любое использование этой функции необходимо строго нормировать, внимательно следить за соблюдением требований защиты и регулярно производить анализ безопасности.

Рассмотрим принципиальные возможности обеспечения безопасности при использовании модуля DISA:

- модуль DISA имеет систему "барьерных кодов". Длина барьерного кода может быть до 11 знаков. Некоторые АТС имеют возможность установить временной график активизации барьерных кодов, то есть некоторый барьерный код может быть активирован только в определенное время определенного дня недели. Может быть установлена конечная дата активизации барьерного кода и число вызовов, которое можно произвести с этим барьерным кодом. Барьерных кодов может быть несколько;

- одновременно со структурой барьерных кодов некоторые АТС могут иметь вышеописанную систему "авторизационных кодов". Длина этого кода также может достигать 11 знаков. В зависимости от авторизационного кода абоненту, закрепленному за этим кодом, могут быть присвоены определенные права. Например, звонить с помощью этого кода только на междугородные номера;

- любая ЦАТС имеет систему выдачи тарификационных данных. В этих данных можно выводить авторизационные коды для определения автора вызовов через модуль DISA;

- некоторые АТС имеют возможность протоколировать номера для всех входящих вызовов. Конечно, эта возможность зависит, во-первых, от функций АТС, во-вторых, от типа подключения АТС к городской телефонной сети.

Рассмотрим методы получения доступа с целью получения конфиденциальной информации, то есть с целью прослушивания абонентов [7].

С развитием цифровых технологий к ранее существовавшим методам прослушивания традиционной телефонии добавляются ранее недоступные методы, использующие новые функциональные возможности цифровой телефонии.

Методы прослушивания (рисунок 1.4), по аналогии с методами ведения переговоров за чужой счет подразделяются на два типа: физический и логический.

Рисунок 4 - Методы несанкционированного прослушивания абонентов

Методы прослушивания конечного абонента на основе физического метода получения доступа традиционны. С подобной возможностью ведется борьба практически со времен появления первой телефонной станции. Подключать устройство прослушивания сообщения можно в любом месте телефонной линии от телефонного аппарата до телефонной станции, а также на самой телефонном станции. Для прослушивания сообщения, передаваемого по телефонной линии, можно использовать любой аналоговый аппарат. С помощью подобных устройств принять информацию можно только тогда, когда соединение абонентов установлено, и они начали вести разговор.

Развитие микроэлектроники породило новые направления в способах перехвата информации - специальные несанкционированные средства (СНС). Такие устройства устанавливают в укромном месте на линию телекоммуникаций. Подключение к линии может быть осуществлено несколькими способами: гальваническим с последовательным или параллельным, включением в линию, индуктивным или емкостным.

Индуктивный и емкостный способы позволяют осуществлять перехват информации, не нарушая целостности покровной изоляции телефонных кабелей.

Защита от таких способов прослушивания может быть осуществлена двумя способами:

- применением организационных и/или конструктивных мер, обеспечивающих невозможность подключения к телефонной линии на всем пути от абонента до абонента (например, положить кабель в стальную трубу и установить сигнализацию, реагирующую на вскрытие трубы; организовать постоянный визуальный контроль за кабелем связи). Это решение влечет за собой значительные капитальные вложения;

- установкой аппаратуры шифрования или скремблеров для каждого абонента.

Для нейтрализации СНС применяют также всевозможные генераторы шума, подавляющие работу передатчиков по эфиру и по линиям в тех диапазонах радиочастот, на которых они работают.

Однако информацию из аналоговой линии можно получить и несколько иным способом. В телефонном аппарате есть несколько специальных акустических преобразователей, предназначенных для преобразования акустических сигналов в электрические и наоборот. Это микрофон и телефон в микротелефонной трубке. Кроме этого, в телефонном аппарате есть электрический звонок или тональное вызывное устройство. Эти устройства предназначены для преобразования электрических вызывных сигналов в акустические, но поскольку в электротехнике все устройства обладают свойством обратимости (правда, с различным коэффициентами преобразования), то и вызывные устройства при воздействии на них акустической волны преобразуют ее в электрический сигнал, пропорциональный воздействующему акустическому сигналу. Эти преобразованные электрические сигналы по различным электрическим цепям

телефонного аппарата попадают в телефонную линию даже в режиме ожидания вызова, то есть при положенной микротелефонной трубке. Величина напряжения преобразованного акустического сигнала достигает 10-20 мВ. Прослушать такой сигнал с помощью наушников телефона или динамика, не применяя низкочастотных усилителей, невозможно, то есть случайное прослушивание сигналов электроакустического преобразования исключено. Однако, для специального прослушивания сигналов электроакустических преобразователей разработаны всевозможные методы пассивного и активного перехвата.

Цифровые станции, пришедшие на смену аналоговым, как будто закрыли проблему простейшего съема информации из телефонной линии. Действительно, подключившись гальванически к цифровому каналу, даже с хорошими усилителями, информации не получишь, но можно услышать сигналы акустоэлектрических преобразователей, которые, к сожалению, в составе телефонного аппарата не только остались, а их стало даже больше. Головка динамика громкоговорящей, связи, микрофон громкоговорящей связи, акустический излучатель вызывного устройства, входные согласующие трансформаторы, кварцевые резонаторы, электролитические конденсаторы - все они в ответ на воздействие на них акустических и виброакустических колебаний создают на своих электрических выводах пропорциональное электрическое напряжение. Эти преобразованные сигналы распространяются по проводникам и элементам телефонного аппарата. Все телефонные аппараты серийного производства для массового применения выполнены без учета явления виброакустических преобразований в элементах телефонного аппарата и без применения специальных способов подавления этих сигналов.

Электрически преобразованный сигнал, "проблуждав" некоторое время в недрах сложнейшей электрической схемы электронного цифрового, аппарата, далее отправляется "путешествовать" по телефонной линии, в

которой он становится наиболее доступен для перехвата ранее описанными способами, с той лишь разницей, что необходимо убрать из принятого сигнала цифровой сигнал, на фоне которого находится в канале преобразованный речевой.

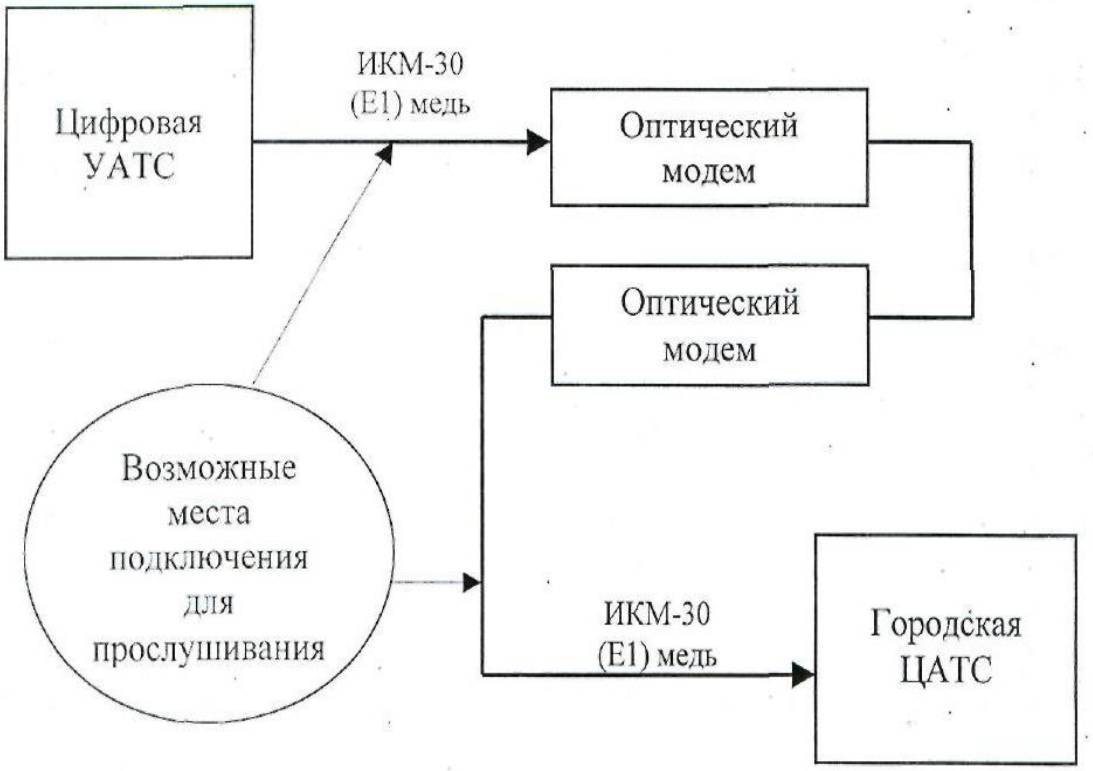


Рисунок 1.5 - Схема стандартного подключения цифровой УАТС к оператору ГТС по потоку E1 (ИКМ-30) с сигнализацией R1.5, R2 EDSS1, ISDN QSIG

Основными методами защиты от подобных подключений являются:

- административное ограничение доступа в помещения, в которых возможно подключения к медным линиям телекоммуникаций;

- установка специализированных устройств, обеспечивающих шифрование;

- административный запрет ведения любых конфиденциальных переговоров с абонентами телефонной сети общего пользования, поскольку гарантировать конфиденциальность при данном типе вызова в принципе невозможно.

При использовании логического метода процесс получения доступа к

ЦАТС для организации прослушивания состоит из двух этапов. Первый этап

- это организация линии связи для самого прослушивания, то есть для установки голосового соединения для передачи собственного звука. Второй этап - получение доступа к управлению ЦАТС для организации несанкционированной конференции между определенными абонентами и организованной предварительно линией связи. Практически все современные телефонные станции имеют для этого необходимый инструментарий. Такова, например, функция "трассировка злонамеренных вызовов". Она предназначена для организации перенаправления вызова, к службе безопасности, записи его и отслеживания всей сопутствующей информации (номер звонящего, номер вызываемого абонента, канал связи, по которому поступил вызов и т.д.). Также используется для прослушивания функция "обеспечение качества обслуживания центров обработки вызовов". В компании, в которой установлен центр обработки вызовов (Call Center), часто бывает необходимо производить анализ качества обработки вызовов (например, как быстро вызовы обрабатываются, как оптимизировать центр обработки вызовов, насколько уважительно работают операторы с клиентами и т.д.).

1.2. Типы нарушителей и мероприятия по защите информации от НСД

Для обеспечения защиты АЛ от НСД необходимо, по крайней мере, четко представлять себе, что необходимо защищать и от кого надо защищаться.

Для разработки эффективной системы защиты ТфОП и ее составных компонентов от НСД необходимо располагать полной и корректной неформальной моделью потенциального нарушителя, в которой должны быть отражены его теоретические и практические знания, возможности, время и место действия и т.п. Под моделью нарушителя в данном случае понимается описание способов и возможностей НСД к услугам телефонной связи [2, 5,

9].

Модель потенциального нарушителя определяет:

- типы (категории) нарушителей;
- цели, которые могут преследовать нарушители каждого типа, возможный количественный состав, используемые технологии, средства и т.п.;
- типовые сценарии возможных действий нарушителей, описывающие последовательность (алгоритмы) и способы их действий на каждом участке АЛ.

В модель потенциального нарушителя следует включать максимально исчерпывающие сведения о действиях внешних и внутренних нарушителей, возможности использования нарушителями каждого определенного сценария и способа действия.

Как указывалось выше, основные причины НСД к услугам телефонной связи обусловлены человеческим фактором. Как показывает практика, преднамеренное происхождение НСП к АЛ обусловливается злоумышленными действиями людей, осуществляемыми в целях реализации НСД к услугам телефонной связи без оплаты.

Предпосылками появления НСП является недостаточная степень защиты АЛ в целом, включая несовершенство физической (конструктивной) защиты компонентов оконечного распределительного оборудования. Виды и способы НСП определяются типом и степенью профессиональной подготовленности нарушителей. Под источником НСП подразумевается сам непосредственный нарушитель.

При анализе потенциальных типов НСП специалистам служб безопасности приходится ставить себя на место нарушителя, для чего необходимо как можно точнее определить (предположить):

- насколько высок уровень профессиональной подготовки нарушителя;

- какой информацией об АЛ он владеет;

- какими разновидностями НСП он воспользуется с наибольшей вероятностью.

По отношению к телефонной линии нарушители могут быть внутренними или внешними. Внутренними нарушителями могут быть лица из числа персонала системы. К этой категории относятся следующие лица:

- операторы системы;

- персонал, обслуживающий технические средства (инженеры, техники);

- администраторы сети;

- эксплутационный персонал и др.

Если рассмотреть абонентский участок (АУ) телефонной линии связи, то к категории внутренних нарушителей могут быть отнесены следующие лица:

- работники учреждений (любого ранга);

- технический персонал, обслуживающий здания (уборщики, электрики, сантехники и т.д);

- руководители различных уровней и т.п.

Внешними нарушителями могут быть любые посторонние лица, не имеющие прямого отношения к данному объекту (зданию, офису, квартире, АЛ и т.д). К этой категории можно отнести следующие лица:

- специализирующиеся на НСД на любом участке АЛ;

- посетители или клиенты организаций, нелегально воспользовавшиеся телефоном в отсутствие его владельца;

- любые лица, случайно или умышленно воспользовавшиеся телефоном без ведома хозяина и т.д.

Злоумышленников можно классифицировать по следующим признакам (рисунок 1.6):

- по уровню знаний;

- по уровню возможностей;

- по длительности и периодичности действия;

- по месту действия;

- по используемым технологиям;

- по используемым средствам.

В настоящее время используются два основных подхода к решению задач обеспечения защиты от несанкционированных подключений:

- индивидуальный подход с последовательным решением частных задач;

- комплексный подход с одновременным решением комплекса задач, направленных на достижение единой цели.

Эффективность защиты АЛ в значительной степени зависит от используемых организационных и технических мероприятий.

Под организационными мероприятиями понимается комплекс мер по регламентации и контролю за использованием абонентской линии. Они проводятся работниками линейных узлов связи, а также индивидуальными абонентами АТС.

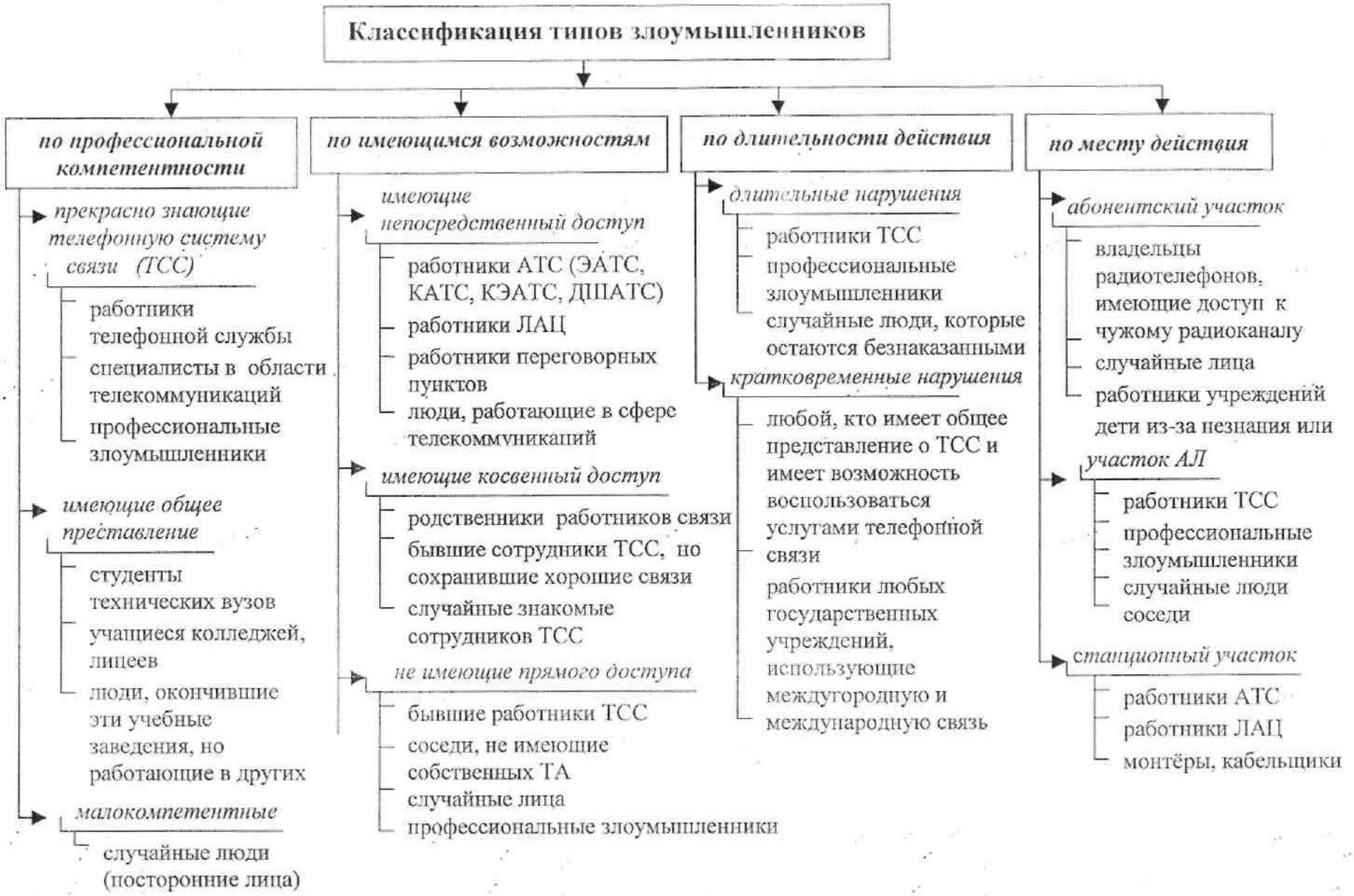


Рисунок 6 - Классификация типов злоумышленников

Ответственность за проведение организационных мероприятий по защите линий телекоммуникаций возлагается в первую очередь на руководителей линейных узлов связи, которые обязаны следить за качеством предоставляемых абонентам услуг. В свою очередь, руководители предприятий, фирм и индивидуальные абоненты, несут ответственность за состояние проводных линий телекоммуникаций, находящихся в пределах занимаемых ими помещений, а также за правильную эксплуатацию оконечных устройств (телефонов, АОНов, факс-модемных аппаратов, автоответчиков и пр.). В организациях, имеющих свои службы безопасности, обязанности по контролю за телефонными линиями и оконечными устройствами разумнее всего возложить именно на них.

Под техническими мероприятиями понимается применение специальных устройств защиты, ограничивающих возможности нарушителей по доступу к линиям телекоммуникаций, которые по воздействию на телефонные линии подразделяются на пассивные и активные.

Пассивные устройства защиты предназначены для регистрации факта подключения и самовольного использования линии. Они не вмешиваются в процесс связи, а только помогают владельцу линии оперативно реагировать на начальный процесс возникновения нелегального использования линии.

Активные устройства защиты предусматривают вмешательство в процесс установления и проведения связи с целью предотвращения реальных финансовых затрат в случаях несанкционированного подключения.

Мероприятия, препятствующие НСД, приведены на рисунке 1.7.

Рисунок 7 – Мероприятия, препятствующие НСД к телефонной линии.

Как указывалось ранее, одним из важных направлений защиты информации является защита от утечки информации через технические

средства. Под утечкой информации понимается ее получение посторонними лицами случайно или преднамеренно без ведома владельцев информации, иначе это называют несанкционированным доступом (НСД), а под обеспечением безопасности информации обычно подразумевают предотвращение НСД.

Все основные методы защиты от утечки информации можно условно разделить на две группы:

- организационные или организационно-технические;

- аппаратные или программно-аппаратные. К первой группе относятся:

- охрана помещений, где размещается аппаратура телекоммуникаций;

- использование приборов, обнаруживающих подслушивающие устройства при НСД к линии телекоммуникаций;

- применение технических средств (фильтров, шумовых генераторов и т.п.), предотвращающих утечку информации по телефонным абонентским линиям и другим каналам побочной утечки информации;

- использование кабелей в герметичной оболочке с контролем разгерметизации при повреждении этой оболочки;

- экранирование кабелей и их зашумление;

- прокладка кабелей в труднодоступных траншеях с устройствами сигнализации о проникновении в них.

Вторая группа позволяет более надежно защититься от утечки информации в каналах телекоммуникаций путем использования аппаратных (аппаратура конфиденциальной связи) и программно-аппаратных (устройство конфиденциальной связи) методов. Таким образом, наиболее эффективными способами предотвращения НСД к линиям телекоммуникаций являются маскирование, скремблирование или шифрование.

2.ОБЩИЕ ПРИНЦИПЫ И МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ В АБОНЕНТСКИХ ЛИНИЯХ ТФОП

2.1 Общие подходы к защите информации в абонентских линиях

В настоящее время при защите абонентских линий от НСД используются следующие способы:

- контроль - за изменениями параметров абонентской линии;

- зашумляющее воздействие на линию;

- управление доступом и контроль за его осуществлением, включая идентификацию/аутентификацию пользователей;

использование обмена сигналами секретного кода между абонентской и станционной частями программно-аппаратного комплекса защиты от НСД;

- анализ параметров активности АЛ при использовании системы повременного учета, которая позволяет осуществлять оперативное выявление попыток НСД;

- использование криптографических методов.

При этом защита АЛ, обеспечиваемая вышеприведенными способами, кроме криптографических, зависит, в основном, от возможностей потенциального нарушителя по технической реализации и сложности алгоритма преодоления используемых механизмов защиты.

В [2],описаны различные устройства, позволяющие контролировать параметры абонентских линий и устанавливать факт несанкционированного подключения к ним. Методы контроля телефонных линий основаны на том, что любое подключение к ним вызывает изменение их электрических параметров: амплитуды напряжения и тока, а также значений емкости, индуктивности, активного и реактивного сопротивления линии. Выполнение требований технической защиты по контролю НСД к АЛ обеспечивается различными индикаторами/анализаторами линий.

Простейшими устройствами обнаружения несанкционированных подключений к АЛ являются всевозможные индикаторы состояния

телефонных линий. Эти устройства устанавливаются на предварительно проверенных телефонных линиях и настраиваются с учетом их параметров. Для проведения углубленных исследований АЛ используются более сложные средства -анализаторы телефонных линий и кабельные локаторы.

Для обеспечения защиты абонентских линий на основе использования обмена сигналами специального кода между абонентской и станционной частями комплекса защиты используются групповые и индивидуальные средства.

Групповые технические средства защиты от НСД обеспечивают:

- поддержку защиты пользователей от НСД к их абонентским линиям;
- ограничение исходящей связи по требованию оператора и/или по заказу абонента;
- определение номера. вызывающего абонента при выполнении междугородних и международных переговоров;
- контроль достоверности информации, выдаваемой аппаратурой АОН.

Индивидуальные средства реализуют нижеследующие методы:

- кодовый доступ к АЛ на основе идентификации/аутентификации пользователей;
- блокировка выхода на межгород;
- запрет параллельного набора и др.

Как показывает международная практика, для индивидуальной технической защиты АЛ от НСД широко используется следующий способ. Каждому абоненту выдается электронная карточка, способная генерировать звуковой сигнал, в котором закодирован индивидуальный код. Электронная карточка после ее активизации пользователем генерирует сигнал частотного набора номера, который используется для идентификации/аутентификации абонента. В случае совпадения индивидуального кода с заранее записанными

данными абоненту предоставляется услуга. Таким образом, эти средства индивидуальной защиты позволяют абоненту самому, управлять с телефона доступом к АЛ, предотвращая тем самым несанкционированный доступ.

2.2. Принципы и методы защиты информации в абонентских линиях

Методы защиты информации в АЛ можно разделить на. две группы [11]: методы, основанные на ограничении физического доступа к линии и аппаратуре связи, и методы, основанные на преобразовании сигналов в линии в форму, исключающую (затрудняющую) для злоумышленника восприятие передачи или искажающую ее содержание.

Методы первой группы в рассматриваемом варианте построения защищенной связи имеют весьма ограниченное применение, так как на основном протяжении линия телекоммуникаций находится вне ведения субъекта, организующего защиту. В то же время, по отношению к аппаратуре терминала и отдельных участков абонентской линии, применение соответствующих мер необходимо.

Ограничение физического доступа предполагает исключение (затруднение):

- непосредственного подключения аппаратуры злоумышленника к электрическим цепям аппаратуры абонентского терминала;
- использования для перехвата информации электромагнитных полей в окружающем пространстве и наводок в отходящих цепях сети питания и заземления;
- получения злоумышленником вспомогательной информации об используемом оборудовании и организации связи, облегчающей последующее несанкционированное вмешательство в канал телекоммуникаций.

Методы второй группы направлены на обратимое изменение формы представления передаваемой информации. Преобразование должно

придавать информации вид, исключающий ее восприятие при использовании аппаратуры, стандартной для данного канала телекоммуникаций. При использовании же специальной аппаратуры восстановление исходного вида информации должно требовать затрат времени и средств, которые по оценке владельца защищаемой информации делают бессмысленным для злоумышленника вмешательство в информационный процесс.

При защите речевого обмена решающее значение имеет форма представления аналогового речевого сигнала в канале телекоммуникаций.

Основные используемые в настоящее время методы преобразования речевого сигнала и их взаимосвязь показана на рисунке 2.1 [11].

Применение вариантов преобразований *Б, В* и, в большинстве случаев, *А* требует наличия соответствующей аппаратуры у каждого из взаимодействующих абонентов сети.

При применении защитного шума (вариант *А)* следует учитывать ряд обстоятельств.

1. Стойкий защитный. эффект оказывает лишь наложение шума, действительно являющегося случайным процессом и по диапазону частот полностью перекрывающего речевой сигнал. В то же время, многие известные и широко применяемые способы получения "шумового" сигнала на самом деле формируют псевдошумовой сигнал, по ряду своих частотных и временных параметров весьма близкий к действительно шумовому, но на самом деле в. значительной степени детерминированный или имеющий существенные внутренние корреляционные связи.

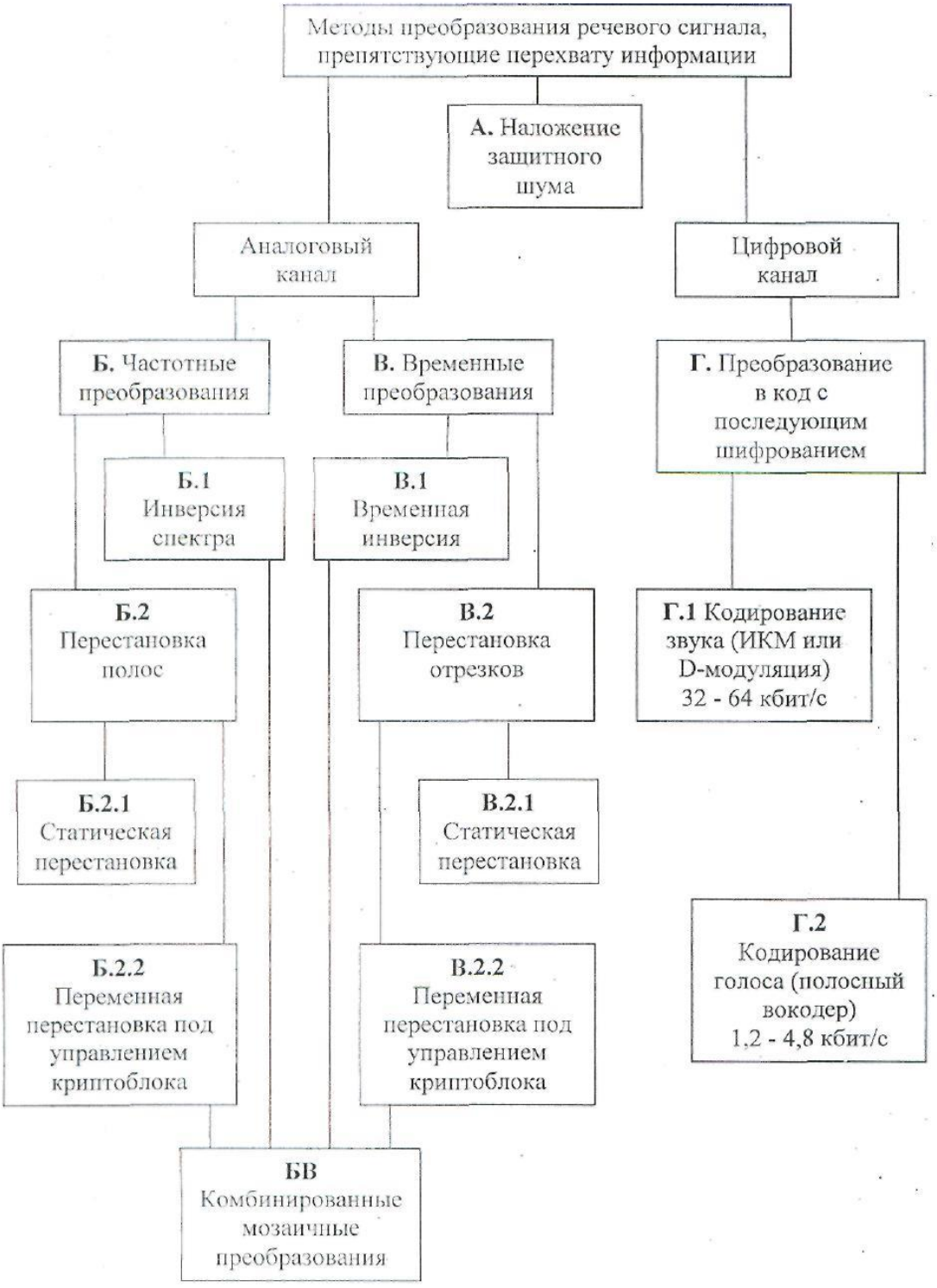


Рисунок 8 - Основные методы преобразования речевого сигнала и их взаимосвязь

Такой сигнал во многих случаях может полностью заменять шумовой сигнал (при измерениях частотных характеристик, оценке

помехозащищенности и пр.). Фактическая детерминированность сигнала, как правило, оказывается даже полезной, поскольку облегчает его параметризацию и стабилизацию. Сигнал, имеющий существенные внутренние корреляционные связи, может быть успешно использован и в качестве защитного шума, если перехват ведется на слух, без использования корреляционной обработки принимаемой или предварительно записанной смеси речевой сигнал/шум.

Однако, при применении относительно несложных методов корреляционной обработки такой "шум" может быть почти полностью подавлен. Следует отметить, что выявить корреляционные связи только по наблюдаемому выходному сигналу используемого генератора довольно сложно. Гораздо проще выявить их, анализируя схему генератора, поэтому, как уже было сказано выше, крайне желательно затруднить получение злоумышленником информации об используемом оборудовании формирования защитного шума, облегчающей последующее его подавление.

2. Речевой обмен в естественных условиях подвержен влиянию множества разнообразнейших помех, а в процессе эволюции речевой и слуховой аппараты человека сформировались в прекрасно сопряженную и исключительно помехоустойчивую систему. Если для технических систем отношение шум/сигнал, необходимое для подавления восприятия сигнала, составляет обычно десятки процентов, то для речи подавление смыслового восприятия происходит при отношении шум/сигнал в несколько сотен процентов, а подавление признаков речи (невозможность фиксации факта разговора) достигается при отношении шум/сигнал близком к 10.

В том же случае, когда "шумовой" сигнал содержит значительную детерминированную составляющую, которая может быть отфильтрована при перехвате, требуемое значение уровня "шума" еще более возрастает. При оценке защитного эффекта шума "на слух" при отсутствии специальных навыков очень легко ошибиться, так как при длительном прослушивании

шума и, тем более, при многократном прослушивании записи выявляются многие элементы речи, невоспринимаемые при кратковременной (в течение нескольких секунд) оценке.

3. Следует учитывать, что и защищаемый речевой сигнал и защитный шум распространяются в пространстве, и обеспечить полную идентичность распределения их в пространстве крайне сложно, поэтому во многих случаях защитный шум может быть в значительной степени подавлен методами направленного или многоканального приема. Хорошо известен даже по бытовой звукозаписывающей технике факт: микрофон надо направить на источник звука, при произвольном же расположении микрофона будет записан не столько нужный звук, сколько окружающие шумы.

Точно также высокое отношение шум/сигнал при одном варианте съема сигнала еще не гарантирует столь же высокую эффективность защитного шума при другом варианте съема сигнала, используемого злоумышленником, а при использовании нескольких специально выбранных точек съема может быть ослаблен защитный эффект большинства источников защитного шумового поля. При этом, конечно, нельзя не учитывать, что применение многоканального приема требует как высокой квалификации злоумышленника, так и значительной свободы его действий по отношению к перехватываемому каналу телекоммуникаций.

Для того, чтобы исключить возможность применения нападающей стороной методов многоканального приема, можно полностью совместить пути распространения защищаемого сигнала и защитного шума, но тогда будет исключено восприятие речи и абонентом, для которого она предназначена. Чтобы выполнить основную задачу - обеспечить связь, можно было *бы* предложить формирование идентичных шумовых сигналов на передающей и на приемной стороне.

При этом на передающей стороне шум складывался бы с' защищаемым

сигналом, а на приемной - вычитался из принимаемого суммарного сигнала. Несмотря на кажущуюся простоту такого варианта, он в течение многих десятилетий не находил реального применения в силу сложности и нестабильности передаточной характеристики канала телекоммуникаций и несовершенства аппаратуры записи и воспроизведения. Компенсация защитного шума на приемной стороне оставалась неполной, причем "остаток" оказывался неприемлемо большим для качественного восприятия речи принимающим абонентом.

Следует отметить, что в настоящее время в связи с развитием методов цифровой записи и воспроизведения звука и методов цифровой фильтрации с применением быстродействующих сигнальных процессоров, позволяющих обеспечить быструю и точную адаптацию к характеристике канала телекоммуникаций, методы защиты, основанные на полном, объединении полезного сигнала и защитного шума в канале телекоммуникаций, могут получить новую жизнь.

Варианты Б, В, БВ изменяют форму (спектр) сигнала в канале, производя перемешивание (скремблирование) отдельных временных или спектральных отрезков исходного сигнала. При этом в линейном сигнале неизбежно сохраняются отдельные обобщенные признаки преобразуемого речевого сигнала, в которых проявляется взаимная связь перемешиваемых отрезков.

Это принципиально, исключает высокую стойкость преобразования. При перехвате сигнала в линии телекоммуникаций при использовании достаточно мощного измерительно-вычислительного комплекса исходная речь может быть восстановлена с приемлемым для смыслового восприятия качеством независимо от примененного закона перестановки, управляющего криптоалгоритма, количества ключей и порядка их ввода.

Варианты В.1, В.2 производят криптографические преобразования цифрового сообщения. Никакие физические признаки исходной речи в

канале телекоммуникаций не обнаруживаются, и степень защищенности определяется только примененным алгоритмом шифрования, размерностью и методом формирования ключа, выполнением правил пользования аппаратурой и ключевой системой.

1. Преобразования с инверсией спектра и статическими перестановками спектральных компонент речевого сигнала (Б.1 и Б. 2.1).

Схемотехническая реализация двух рассматриваемых вариантов заметно отличается, что и обусловливает их раздельное рассмотрение. Однако с точки зрения достигаемых результатов по защищенности сигнала в канале телекоммуникаций оба варианта аналогичны.

Процесс инверсии спектра сигнала при передаче и его восстановления при приеме иллюстрируется на рисунке 2.2.

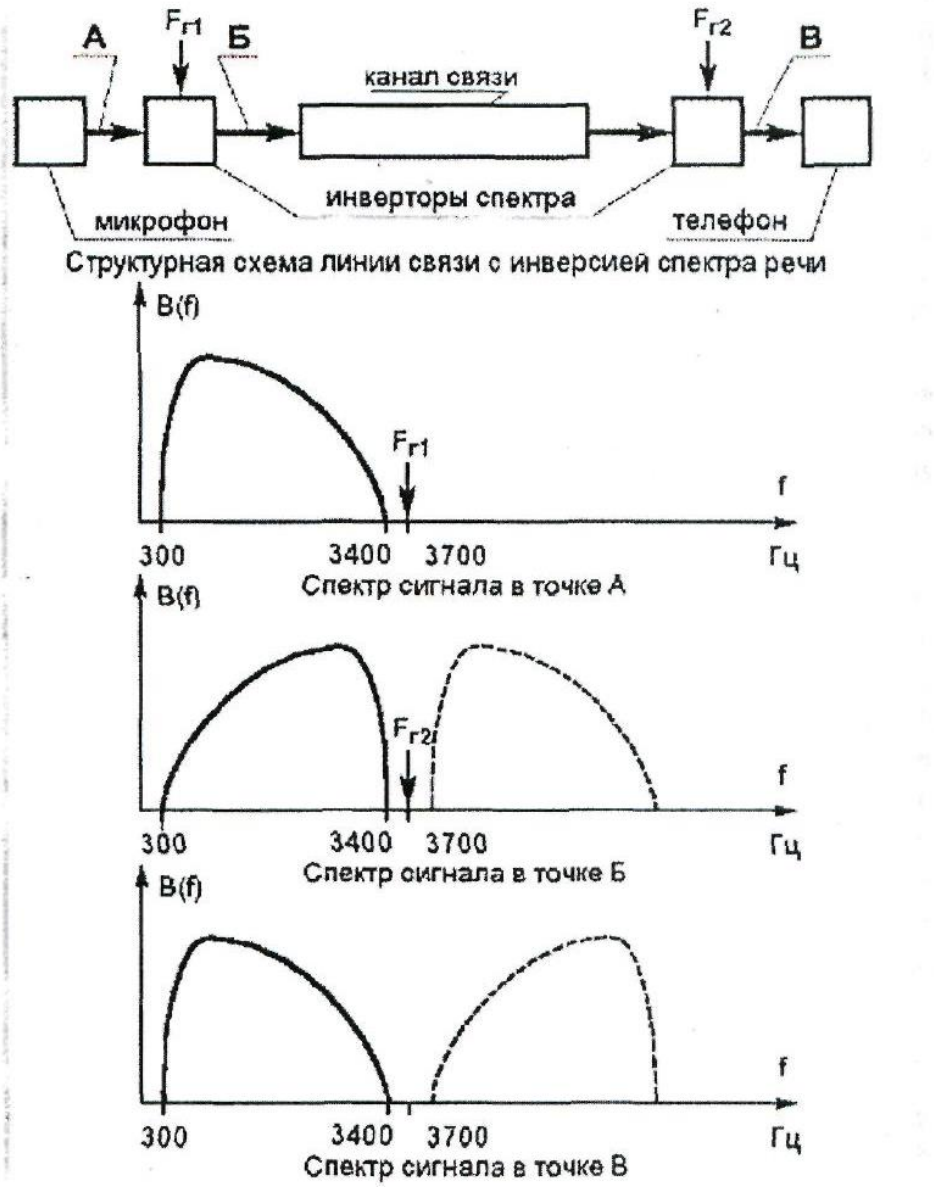


Рисунок 9 - Процесс инверсии и восстановления спектра сигнала

Схема инвертора представляет собой балансный смеситель. При частоте гетеродина Fr, равной сумме граничных частот Fн и Fв преобразуемого сигнала (3700 Гц для стандартного телефонного канала с Fn = 300 Гц и Fe = 3400 Гц) нижняя полоса частот после смесителя воспроизводится в исходной полосе частот, то есть в полосе канала в инверсном виде. При приеме производится повторная инверсия и исходный сигнал восстанавливается.

Качество восстановленной речи зависит от качества (на передающей и на приемной сторонах) смесителей, фильтров, ограничивающих спектр входного сигнала и выделяющих нижнюю полосу частот преобразованного,

сигнала, а также от коррекции на приемной стороне частотных искажений канала, влияние которых также сказывается инверсно: затухание канала в высокочастотной части спектра на приеме сказывается в низкочастотной части сигнала и наоборот.

При перехвате сигнал с инвертированным спектром может быть легко восстановлен любым аналогичным аппаратом (не обязательно однотипным), а при соответствующей тренировке - воспринят человеком непосредственно..

Для повышения стойкости защиты некоторые изготовители вводят переменную частоту гетеродина, устанавливаемую партнерами по договоренности в форме числового кода-пароля, вводимого в аппарат при переходе в защищенный режим.

Возможности такого дополнительного частотного сдвига, приводящего к несовпадению спектра передаваемого сигнала и номинальной , частотной полосы канала телекоммуникаций и, соответственно, к ухудшению качества восстановленной речи, ограничены несколькими сотнями герц. Достигаемый эффект весьма условен. Действительно, при прослушивании восстановленного сигнала, в случае неравенства частот гетеродинов на передаче и на приеме, в первый момент возникает ощущение неестественной и непонятной речи, которое, однако, почти не мешает воспринимать ее смысл после некоторой адаптации.

Процесс преобразования с фиксированными перестановками спектральных компонент речевого сигнала при передаче и его восстановления при приеме иллюстрируется на рисунке 2.3.

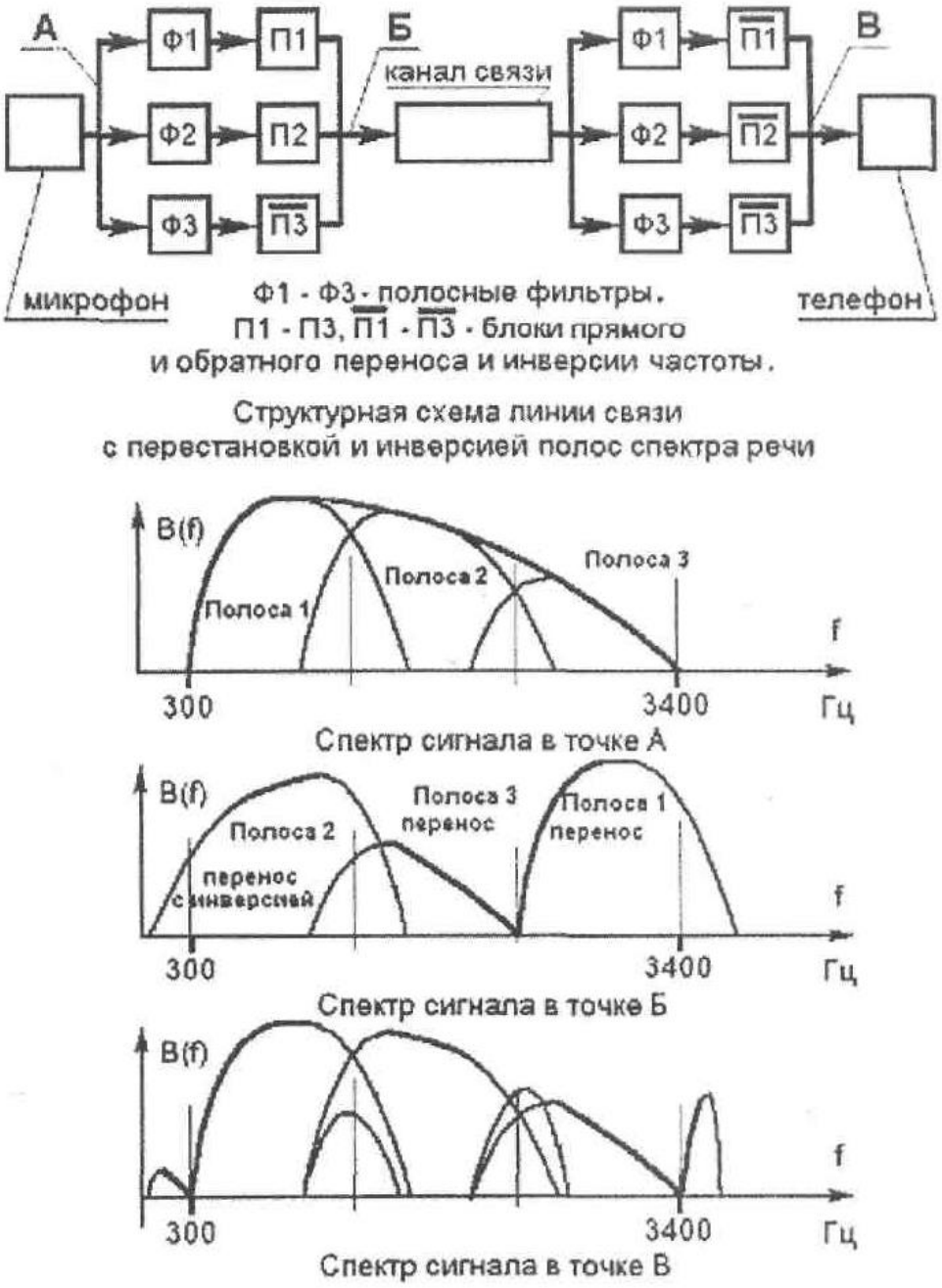


Рисунок 10 - Процесс преобразования и восстановления спектральных компонент речевого сигнала

При таком преобразовании разборчивость речевого сигнала нарушается в значительно большей степени, чем при простой инверсии. Следует, однако, учитывать, что выбор вариантов частотных перестановок весьма ограничен. Фильтры, выделяющие частотные полосы в исходном и в линейном сигнале, имеют конечную крутизну характеристики, в результате чего на заметном

частотном интервале в окрестности границы частотных полос будет происходить заметное невосстановимое смешение различных компонент сигнала. Полная полоса частот (300 - 3400) Гц составляет 3,5 октавы. При формировании трех полос (по 1,2 октавы на каждую полосу) при использовании фильтров восьмого порядка (нарастание затухания около 48 дБ/октаву) затухание в середине (!) соседней полосы составит не более 30 дБ, что предопределяет низкое качество восстановленной речи. Существенное увеличение порядка фильтров настолько усложняет аппаратуру, что она теряет преимущества перед другими вариантами преобразователей. В тоже время, число возможных перестановок из трех полос - всего лишь 6, из четырех полос - 24, то есть даже в условиях прямого перехвата, не говоря уже об анализе записи, подбор нужной подстановки не составит труда.

Наиболее существенным положительным качеством рассматриваемых преобразователей (Б.1 и Б.2.1) является их автономность, то есть отсутствие необходимости во взаимной синхронизации передающего и приемного аппарата и, соответственно, отсутствие задержки связи на время проведения синхронизации и возможных срывов защищенного режима из-за качества канала, недостаточного для проведения синхронизации. Если удалось установить связь в открытом режиме после включения партнерами инверторов, будет реализован и защищенный режим.

Положительными качествами такой аппаратуры также являются:

- дешевизна;

- возможность построения схем, не вносящих задержку сигнала;

- малая критичность к качеству используемого канала телекоммуникаций и предельная простота в управлении.

Аппаратура может включаться между телефонным аппаратом и линией в стандартный двухпроводной стык между телефонным аппаратом и микротелефонной трубкой, может использоваться в виде накладки на микротелефонную трубку с акустической передачей преобразованного

сигнала. Переход в защищенный режим происходит по взаимной договоренности партнеров после установления соединения. Переход происходит немедленно после нажатия соответствующей клавиши (или другого управляющего действия). Включение и выключение защищенного режима осуществляется каждым партнером самостоятельно, синхронизация действий не требуется.

При разговоре в линии прослушивается характерный сигнал, по структуре полностью повторяющий передаваемую речь. Восстановленный сигнал имеет высокое качество. В дешевых аппаратах с недостаточной фильтрацией возможно наличие свистящих тонов и изменение тембра голоса говорящего. Наличие посторонних шумов в помещении, из которого ведется передача, сказывается на качестве восстановленного сигнала так же, как в открытом режиме, на стойкость защитного преобразования почти не влияет.

2. Преобразования с временными перестановками (скремблированием) и временной инверсией элементов речевого сигнала со статическим законом перестановки (В.1, В.2.1.)

Принцип работы аппаратуры сходен с разрушением и последующим восстановлением мозаичной картины, что обусловило появление названия "аппаратура мозаичных преобразований".

Данный класс аппаратуры требует наличия в своем составе блока запоминания сигнала с управляемым доступом по записи и считыванию. Временная перестановка элементарных отрезков речевого сигнала и восстановление их последовательности на приеме занимают соответствующий интервал времени, поэтому обязательным свойством такой аппаратуры является заметная задержка сигнала на приемной стороне.

Процессы преобразования сигнала показаны на рисунке 2.4.

Чем меньше длительность, элементарных отрезков, на которые разбивается исходный речевой сигнал и чем больше элементов участвуют в операции перестановки, тем сложнее процесс восстановления речи по

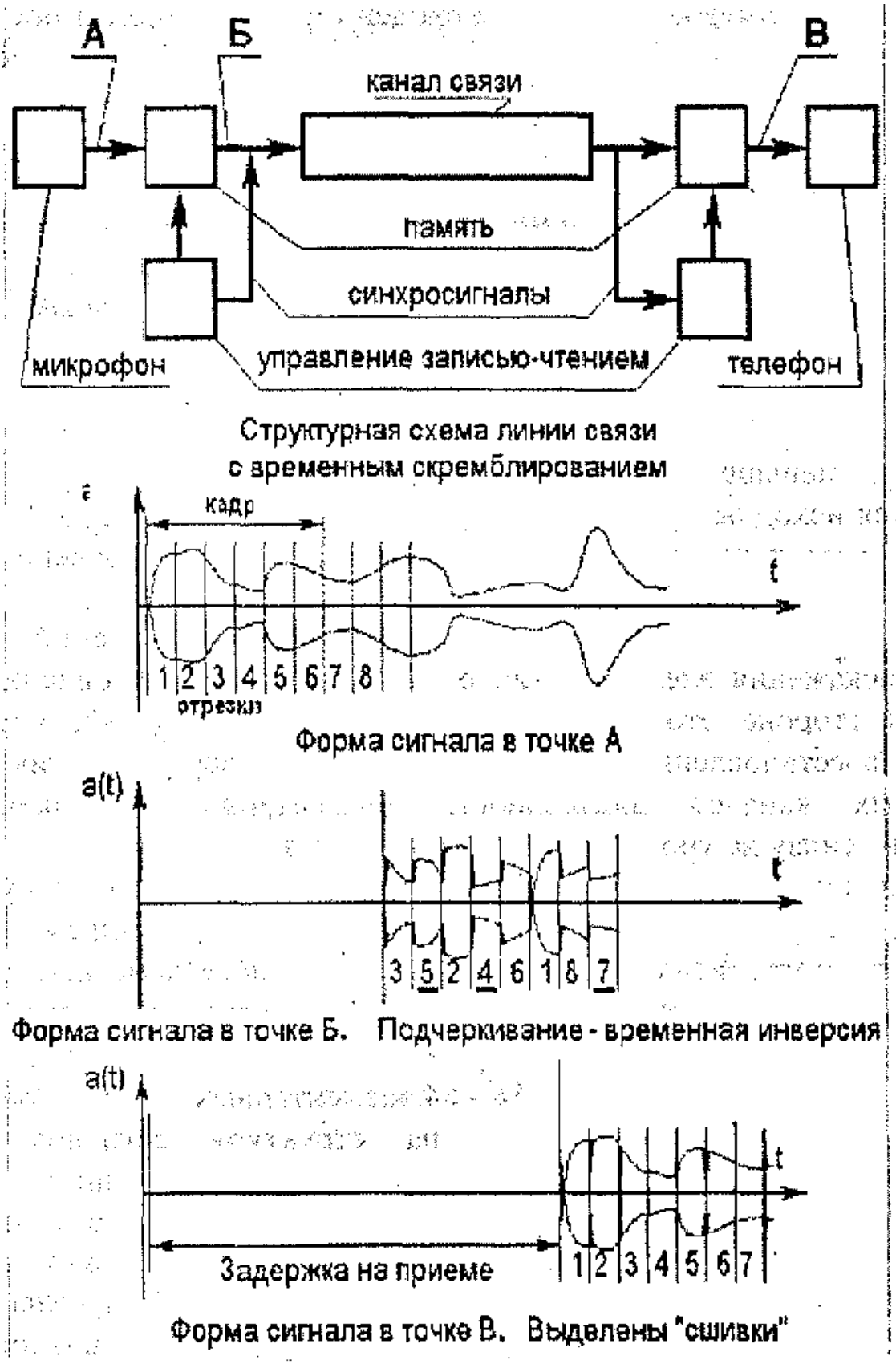


Рисунок 11 - Процессы преобразования сигнала

перехваченному линейному сигналу.

Однако при передаче по каналу телекоммуникаций возникают краевые искажения элементарных отрезков. При восстановлении речи на приемной стороне это приводит к появлению "сшивок", ухудшающих качество восстановленного сигнала. С учетом характеристик реальных телефонных каналов длительность элементарных отрезков сигнала ограничена снизу на уровне 15-20 миллисекунд.

Увеличение числа перемешиваемых элементов мозаики - увеличение "глубины перестановки" - ограничено возрастанием задержки восстановленного сигнала на приеме. При диалоге заметные неудобства возникают при задержке более 0,3 секунды, а при задержке более 1 секунды диалог становится невозможным. Оба указанных фактора определяют глубину перестановки на уровне 16-64 элементарных отрезков речи.

Маскирующее воздействие на структуру сигналов в линии телекоммуникаций может быть достигнуто временной инверсией (воспроизведением в обратном направлении по отношению к записи) всех или отдельных отрезков. Такое преобразование неэффективно на коротких отрезках (с продолжительностью менее длительности одного элементарного звука речи). Применение длинных отрезков уменьшает возможность их перемешивания, поэтому временная инверсия применяется исключительно как дополнительное преобразование в комбинации с временными перестановками. При этом наиболее эффективна временная инверсия всех отрезков.

Временные перестановки и временная инверсия при правильном выборе параметров перестановки исключают непосредственное прослушивание речи в канале телекоммуникаций, но при анализе записи или при оперативном анализе сигнала на месте перехвата статическая перестановка, повторяющаяся из кадра в кадр, легко выявляется по спектральным и амплитудным связям отрезков, в результате чего исходная речь может быть

восстановлена с применением несложной аппаратуры (ПЭВМ с аудиоплатой).

В то же время, по своему составу и сложности алгоритма аппаратура с фиксированными перестановками незначительно отличается от аппаратуры с переменными перестановками, управляемыми криптоблоком, поэтому в настоящее время для целей защиты информации применяются почти исключительно аппараты с переменными перестановками.

3. Преобразования с временными или частотными перестановками (скремблированием) с переменными перестановками под управлением криптобпока и комбинированные мозаичные преобразования (Б.2.2, В.2.2, БВ).

Применение переменных перестановок позволяет значительно затруднить восстановление исходной речи при перехвате сигнала в канале. При правильном выборе криптоалгоритма удачный подбор перестановки на одном интервале никак не способствует подбору перестановок на последующих интервалах. Кроме того, введение криптоалгоритма с индивидуальным ключом исключает возможность использования для перехвата однотипного аппарата.

Аппаратура строится, как правило, на базе сигнальных процессоров, имеет в своем составе аналого-цифровые (АЦП) и цифро-аналоговые (ЦАП) преобразователи, криптоблок управления перестановкой, систему ввода или формирования ключа. Обязательным этапом рабочего процесса является начальная синхронизация взаимодействующих аппаратов и их последующая подсинхронизация.

При переходе в защищенный режим по договоренности абонентов возникает интервал прерывания речевой связи, который занимает процесс синхронизации и установления взаимодействия криптоблоков. В ряде изделий в это же время абонент, используя тастатуру телефонного аппарата или тастатуру скремблера, или персональный узел памяти, должен ввести

ключ. В результате, переход в защищенный режим может занимать до 10 -20 секунд. При этом надо учитывать, что при плохом качестве канала синхронизация и переход в защищенный режим могут не состояться, хотя связь в открытом режиме, пусть и при плохом качестве, поддерживается.

Наличие временной задержки при передаче сигнала при работе по двухпроводной линии неизбежно приводит к возникновению "эха" (это же характерно и для статических временных перестановок). В современной аппаратуре телекоммуникаций отработаны весьма совершенные алгоритмы

подавления эха, широко применяемые в скоростных модемах. Однако человеческое ухо реагирует на уровни эхо-сигналов, заведомо несущественные для модемов, поэтому даже в наиболее удачных моделях скремблеров подавление эха до не замечаемого абонентом уровня достигается только при случайном удачном сочетании параметров линии телекоммуникаций.

Криптоблок, управляющий процессом перестановок, может использовать как симметричную, так и несимметричную ("с открытым ключом") ключевую систему. Варианты с несимметричной системой предпочтительнее, так как упрощают эксплуатационный процесс и исключают вскрытие записи при хищении личного ключа. Однако и в этом случае применение личного пароля полезно, так как исключает вхождение в связь посторонних лиц.

Учитывая то вышеуказанное обстоятельство, что и при самом, совершенном криптоалгоритме передаваемая речь может быть восстановлена при перехвате линейного сигнала по остаточным признакам взаимного расположения элементарных отрезков, применение. в скремблерах очень мощных криптоалгоритмов и ключевых кодов большой длины не оправдано. Вполне достаточной является длина ключевого кода порядка 9 десятичных (30 двоичных) знаков в симметричной ключевой системе и 30 десятичных (около 100 двоичных) - в несимметричной ключевой системе.

При разговоре в линии прослушивается характерный "рваный" сигнал, в котором достаточно. легко определяется структура передаваемой речи. Восстановленный сигнал имеет высокое качество, мало отличающееся от качества речи в открытом режиме на том же канале. Наличие посторонних шумов в помещении, из которого ведется передача, сказывается на качестве восстановленного сигнала так же, как в открытом режиме. Однако ритмические помехи, создающие "шкалу времени" параллельную, преобразуемому сигналу, могут повлиять на стойкость защитного преобразования.

Аппаратура может включаться между телефонным аппаратом и линией в стандартный двухпроводной стык между телефонным аппаратом и микротелефонной трубкой, может использоваться в виде накладки на микротелефонную трубку с акустической передачей преобразованного сигнала.

Таким образом, основными положительными качествами аппаратуры мозаичных преобразований - скремблеров являются:

- относительно высокая стойкость защиты передаваемого речевого сигнала, исключающая его непосредственное прослушивание даже при наличии группы высокотренированных аудиторов и требующая для. восстановления речи значительных затрат времени при использовании специализированных измерительно-вычислительных комплексов,

применяемых государственными спецслужбами;

- относительно низкая стоимость;

- простота эксплуатации (для моделей, специально разработанных для непрофессионального пользователя).

К недостаткам данного класса аппаратуры следует отнести:

- задержку восстановленного сигнала на приемной стороне, требующую привыкания и затрудняющую диалог;

- наличие эха, зависящего от параметров коммутируемой линии

телекоммуникаций;

- задержку связи на время прохождения процесса синхронизации аппаратов;

- возможность срыва синхронизации на плохих каналах.

По совокупности качеств этот класс аппаратуры представляется наиболее приемлемым для использования в корпоративных системах защищенного обмена речевой информацией оперативного характера, не требующей длительного периода секретности.

4. Аппаратура защиты с кодированием звука на скорости 30-64 кбит/с с последующим шифрованием цифрового потока.

Этот класс аппаратуры защиты речевого обмена информацией представляется наиболее перспективным в предположении широкого внедрения каналов, обеспечивающих устойчивую модемную связь на скорости 32 кбит/с. Для оцифровки речевого сигнала производятся массовые и дешевые "кодеки". Для выполнения операции шифрования на скорости 32 кбит/с достаточно вычислительной мощности наиболее дешевых микропроцессоров, элементная база модемов также достаточно отработана и дешева.

Для вхождения в режим защищенной связи взаимодействующим аппаратам требуется некоторое время для синхронизации криптоблоков и обмена служебными криптопосылками. Однако, при скорости обмена не менее 32 кбит/с необходимое для этого время в самых тяжелых допущениях не превышает 1 секунды. Задержка восстановленной речи на приемной стороне практически отсутствует. Качество речи, восстановленной после расшифрования линейного сигнала, не отличается от качества открытой речи. Стойкость защиты полностью определяется применяемым криптоалгоритмом и практически не ограничена. Сигнал в канале не несет никаких признаков защищаемого сигнала, прослушивается как обычный сигнал модема соответствующей скорости. Может быть применена как

симметричная, так и несимметричная ключевая система, причем при скорости обмена 32 кбит/с дополнительный обмен информацией между криптоблоками, необходимый для формирования несимметричных ключей, не потребует существенного времени.

5. Аппаратура защиты с кодированием голоса (полосный вокодер или липредер) на скорости 1200 - 4800 бит/сек с последующим шифрованием цифрового потока.

Аппаратура такого типа составляет основу государственных систем защищенной речевой связи во всех странах мира.

Первые работы по созданию вокодерной аппаратуры этого типа относятся к концу сороковых, началу пятидесятых годов прошлого века.

Принцип работы аппаратуры основан на ограниченности набора звуков, формируемых голосовым аппаратом человека в процессе нормального речевого обмена. Это позволяет поставить задачу распознавания характерных звуков и кодирования их при относительно низкой скорости цифрового потока. Оцифровка звука на скорости 30-60 кбит/с позволяет достаточно хорошо описать любой слышимый звук - шумы, музыку, голос. Если довести распознавание звуков до смыслового уровня, будет получен некоторый эквивалент печатного текста, не несущий никаких индивидуальных характеристик голоса и интонаций, но соответствующий минимальной скорости цифрового потока, зависящей только от скорости чтения текста. Исследование структуры звука человеческого голоса показало, что для передачи не только текста, но и индивидуальности голоса, его интонаций, тембра достаточно скорости цифрового потока 2-5 кбит/с, а при некоторой потере качества речи и 1 кбит/с.

При такой скорости передача цифрового потока может быть обеспечена практически по любому каналу телефонной связи. Это ставит аппаратуру защиты речевой связи с вокодерным преобразованием речи в исключительное положение, так как обеспечивается организация

защищенной речевой связи с любым абонентом, который имеет открытую телефонную связь, а шифрование цифрового потока позволяет обеспечить любую заданную стойкость защиты.

К сожалению, применение такой аппаратуры ограничивается двумя факторами. Во-первых, алгоритм кодирования звуков человеческого голоса очень сложен и даже при применении наиболее совершенных сигнальных процессоров использует все их вычислительные ресурсы. Как следствие, аппаратура оказывается дорогой, при сопоставимых условиях в 10-20 раз дороже скремблера. Во-вторых, высокая стойкость защиты, обеспечиваемая такой аппаратурой, повлекла за собой правовые ограничения на ее применение.

Из особенностей такой аппаратуры можно отметить следующее. Процесс анализа речи на передающей стороне принципиально требует интервала времени не менее десятка миллисекунд (типичный интервал анализа 15-30 мс), поэтому на приемной стороне восстановленная речь несколько задерживается, но задержка эта значительно меньше, чем у скремблера, и для непредвзятого слушателя незаметна.

Поскольку алгоритм анализа настроен на максимальное использование особенностей звучания некоторого среднего человеческого голоса, при произнесении необычно высоких звуков и при некоторых звукосочетаниях процесс кодирования может нарушаться и в восстановленной на приемной стороне речи возникают характерные "призвуки".

По той же причине различные шумы (в частности, другие голоса) на передающей стороне могут существенно сказываться на качестве речи на приемной стороне. Кодирующий блок все звуки пытается представить как компоненты речи одного лица, что может привести к заметным искажениям. Например, если на микрофон подействует чисто механический шум, после кодирования и декодирования он может превратиться во вполне человеческий голос. Это обстоятельство накладывает определенные

ограничения на условия переговоров с использованием вокодерной аппаратуры.

2.3 Средства защиты информации в абонентских линиях

Как указывалось ранее, для защиты телефонных сообщений применяют два принципиально различных метода - преобразование аналоговых параметров речи и цифровое шифрование [13-16].

При аналоговом скремблировании изменяются характеристики исходного речевого сигнала таким образом, что результирующий сигнал становится неразборчивым, но занимает ту же частотную полосу. Это дает возможность без проблем . передавать его по тем же каналам телекоммуникаций, что и обычную речь. При использовании этого способа закрытия сообщений речевой сигнал может подвергаться следующим преобразованиям:

- частотная инверсия;
- частотная перестановка;
- временная перестановка.

В значительном количестве изделий до сих пор применяется инверсия частотного спектра. Известно, что при гетеродинном способе преобразования сигнала на выходе преобразователя сигнал имеет частотный спектр, представленный на рисунке 2.5.

Вся информация сосредоточена в боковых полосах слева и справа от несущей частоты. В передающем устройстве одна из полос подавляется фильтром, а другая усиливается и подается в канал телекоммуникаций. Если взять сигнал, который будет иметь инвертированный спектр, то любой подключившийся к линии человек не сможет разобрать этот сигнал. Собеседник, которому адресовано это сообщение, примет его нормально, так как его приемник преобразует сигнал с инвертированным спектром в нормальный сигнал

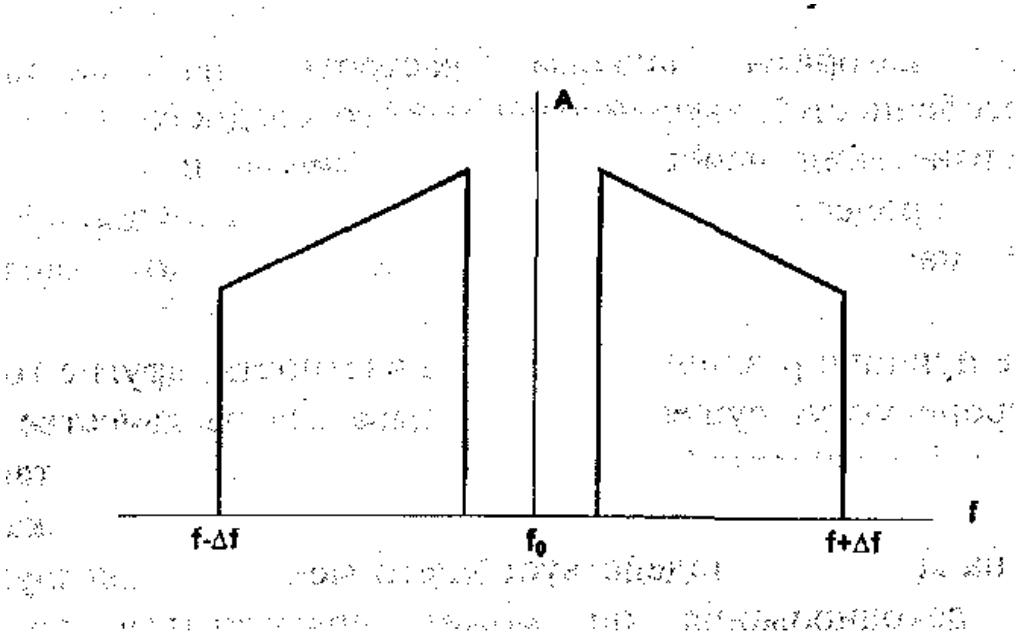


Рисунок 12 - Спектр преобразованного сигнала

В более сложных системах речь дробится на определенные, равные по длительности временные участки (интервалы коммутации) продолжительностью от 0,2 до 0,6 с. В пределах этого участка происходит дополнительное дробление на более мелкие участки длительностью (30 - 60) мс. Всего таких маленьких участков речи может быть от нескольких единиц до нескольких десятков. Эти информационные мелкие участки до передачи в линию телекоммуникаций запоминаются в каком-либо запоминающем устройстве, "перемешиваются" между собой по какому-либо закону, после чего перемешанный таким образом сигнал передается в канал телекоммуникаций. На приемном конце канала телекоммуникаций, где закон перемешивания известен, осуществляется обратный процесс "сборки" нормального сигнала (рисунок 2.6).

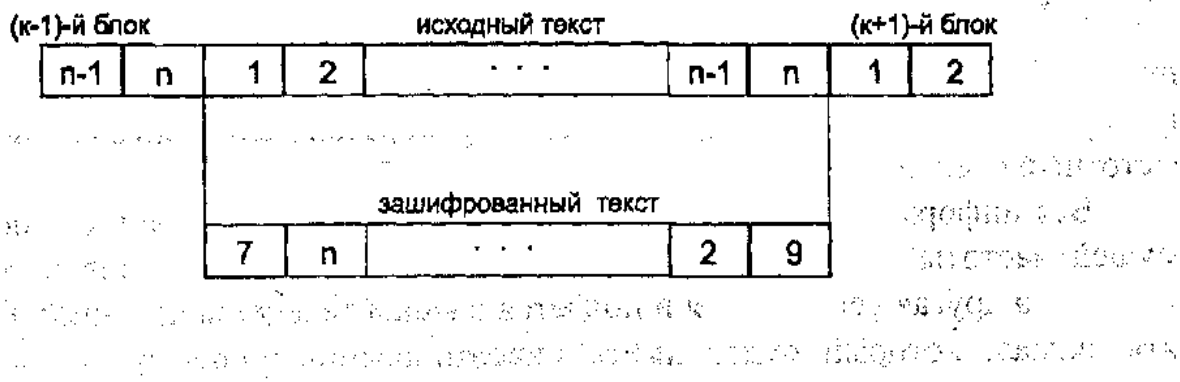


Рисунок 13 - Скремблирование методом временной перестановки

К преимуществам этого вида закрытия относится сравнительная простота технической реализации устройства, а, следовательно, низкая стоимость и малые габариты, возможность передачи зашифрованного речевого сигнала по стандартному телефонному каналу и хорошее качество восстанавливаемого исходного сигнала. Главным недостатком этого способа является его низкая стойкость к несанкционированному восстановлению. В связи с тем, что сигнал является непрерывным, у криптоаналитика после записи и выделения участков (а это легко сделать, так как в линии телекоммуникаций присутствует сигнал, определяющий начало участков) появляется возможность осуществить дешифрование даже без знания примененной системы ключей.

Такой способ закрытия информации применяется только в тех случаях, когда информация не является слишком ценной и когда ее значимость теряет свою актуальность через относительно небольшой период времени.

Более стойкое закрытие информации получается, когда тот же принцип дробления и перемешивания применяется в отношении частотного диапазона сигнала. В этом случае с помощью системы фильтров вся полоса частот стандартного телефонного сигнала делится на некоторое количество частотных полос, которые перемешиваются в заданном порядке. Как правило, такое перемешивание осуществляется по псевдослучайному закону,

реализуемому генератором ключа. Перемешивание частотных полос осуществляется со скоростью (2 - 16) циклов/с, то есть одна перестановка длится (60 - 500) мс, после чего она заменяется следующей. Перемешивание частотных поддиапазонов осуществляется либо в прямом, либо в инверсном виде. В процессе разговора кодовые комбинации могут меняться с некоторой цикличностью, однако при этом должна осуществляться синхронизация. Принцип частотных перестановок приведен на рисунке 2.7.

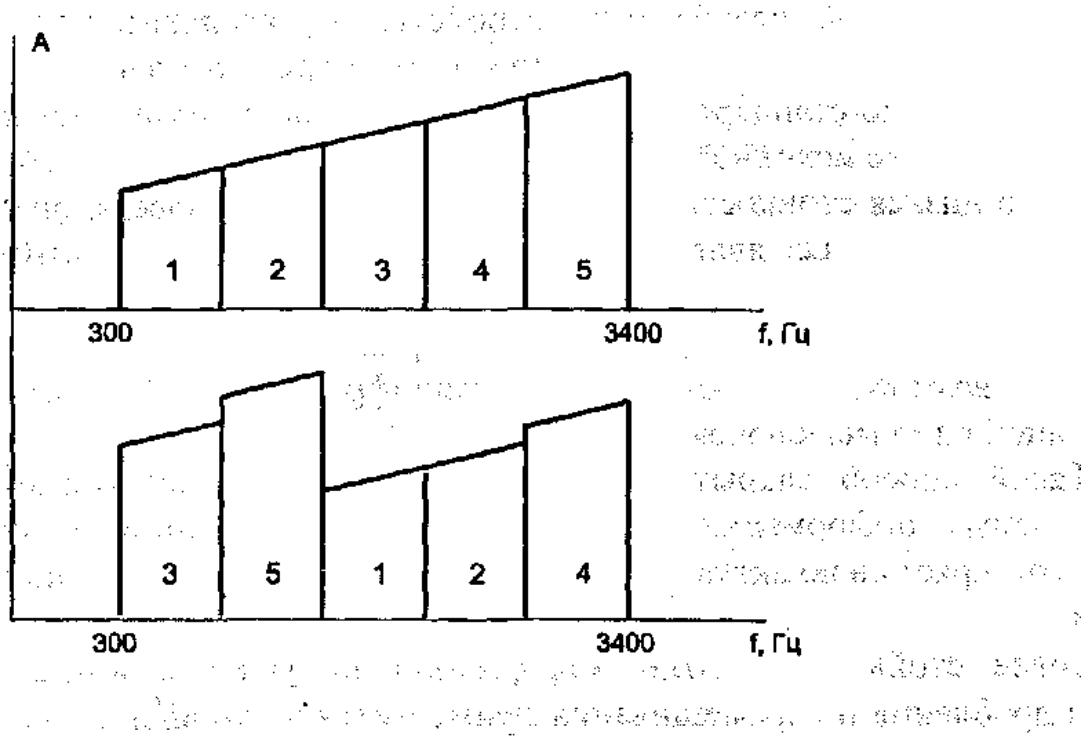


Рисунок 14 - Пример скремблирования методом частотной перестановки

Наиболее высокий уровень стойкости при аналоговом закрытии речи получается с помощью объединения двух вышеуказанных способов. При этом временные перестановки разрушают смысловой строй, а частотные преобразования перемешивают гласные звуки. Число частотных полос обычно берется равным 5-6.

Временной способ обработки используется в аппаратуре TRS769 (компании Thomson-CSF). При этом производится запись речевого сигнала в память с последующим преобразованием выборок из 24 миллисекундных сегментов, которые, в свою очередь, рассеиваются в псевдослучайной

последовательности с образованием 14 групп. Далее сигнал объединяется с обратным псевдослучайно распределенным спектром сигнала, что еще больше защищает исходное сообщение. Амплитуды сегментов речевых сигналов поддерживаются на уровне ниже среднего уровня обычных звуков речи.

Применение такого метода позволяет создать полную неопределенность относительно положения по времени каждого сегмента, повышая тем самым степень закрытости системы. Кроме того, закон, управляющий временной обработкой речевого сигнала, меняется от сегмента к сегменту неповторяющимся и непредсказуемым способом, поскольку он контролируется сигналами псевдослучайной последовательности.

При выборе скремблера следует обращать внимание не столько на число возможных ключевых комбинаций, сколько на сложность преобразований, которые в нем применены.

В простейших скремблерах, защищающих лишь от прямого прослушивания, используются только частотные перестановки и инверсии (число каналов не превышает 4, интервалы коммутации - постоянная величина).

В скремблерах среднего класса, обеспечивающих стойкость в течение нескольких часов, применяются частотно-временные перестановки с числом частотных каналов от 5 до 10.

В сложных скремблерах, обеспечивающих стойкость в течение нескольких дней, должны быть переменными интервалы коммутации, использоваться частотно-временные перестановки с большим (более 10) количеством частотных каналов и переставляемых временных интервалов. Число возможных ключевых комбинаций должно быть более 10. Следует обращать внимание на то, какой вид связи поддерживает скремблер: симплексный (передача информации только в одном направлении);

полудуплексный (поочередный обмен информацией); дуплексный (одновременный двунаправленный обмен).

При цифровом способе закрытия речевой непрерывный сигнал предварительно преобразуется в дискретный вид. Любой непрерывный сигнал может быть без потери информации заменен последовательным набором мгновенных значений этого сигнала, если эти значения сигнала берутся с частотой, не менее, чем в два раза превышающей самую высокочастотную составляющую этого сигнала (согласно известной теореме Котельникова). Для стандартного телефонного канала это означает, что такое стробирование сигнала должно происходить с частотой не менее 6 кГц, так как верхняя частотная составляющая телефонного сигнала ограничивается частотным пределом стандартного телефонного канала 3,4 кГц.

Максимальное расстояние между точками отсчета на временной оси (xl, т2, т3, ...) не должно превышать T=1/2F, где F - максимальная частотная составляющая непрерывного сигнала. В этом случае непрерывная кривая полностью описывается последовательностью значений Ai и временным интервалом At. Если эти значения представить в виде набора чисел, то эти числа можно зашифровать любым известным способом. В этом случае способ цифрового шифрования является универсальным, и в настоящее время имеются такие типы шифраторов, которые могут шифровать все виды передаваемой информации - от буквенно-цифровой до изображений. При этом любая информация предварительно преобразуется в цифровую форму. В канал телекоммуникаций выдается набор дискретных знаков (как правило, единиц и нулей).

Такое шифрование имеет некоторые особенности. Первая - это требование быстрой выработки огромного количества знаков шифра, естественно, при сохранении его высокого качества. Например, если имеется 6000 мгновенных значений сигнала в любую секунду, а динамический диапазон равен 20 дБ (это означает, что максимальная амплитуда сигнала в

10 раз больше его минимального значения), то в одну секунду нужно иметь не менее 6000 х 4 = 24000 двоичных знаков шифра (в двоичной системе счисления для представления числа 10 нужно четыре двоичных знака), то есть скорость выдачи шифра и передачи в линию в этом случае должна быть не менее 24 кбит/с, что достаточно проблематично осуществить по стандартному телефонному каналу.

Следовательно, второй особенностью при цифровом шифровании речевого сигнала является требование наличия гораздо более широкой полосы канала для передачи двоичного сигнала шифропоследовательности. Это означает, что такой сигнал уже не удастся передать по стандартному телефонному каналу. Данное серьезное ограничение накладывает свои особенности на применение цифрового шифрования речевого сигнала по такой схеме.

Использование специфичных характеристик речевого сигнала и применение различных технических и математических способов позволяет резко сузить требуемую полосу и передать зашифрованный цифровым способом преобразованный речевой сигнал по стандартному телефонному каналу.

Чаще всего для преобразования речевого сигнала используется вокодер - устройство, выделяющее существенные параметры речи и преобразующее их в цифровую форму. Однако в этом случае, хотя речь и сохраняет требуемую разборчивость, опознать своего собеседника по тембру голоса практически невозможно, так как голос синтезируется речевым синтезатором и имеет "металлический" оттенок. Качество речевого сигнала будет весьма высоким только в том случае, если для сигнала, зашифрованного цифровым способом, использовать канал с широкой полосой (УКВ или радиорелейную связь).

Для нормальной работы устройств защиты информации на отечественных телефонных каналах скорость передачи информации на выходе криптоблока, а значит и вокодера, не должна превышать 4800 бит/с.

При этом слоговая разборчивость достигает 99 % при удовлетворительной узнаваемости абонента. Телефонный канал среднего качества обеспечивает слоговую разборчивость порядка (85-88) %.

При цифровом шифровании речевого сигнала сложной проблемой (вследствие высоких скоростей передачи информации) является и проблема ввода ключей, а также проблема шифросинхронизации. Важно добиться того, чтобы шифраторы на приемном и передающем концах линии телекоммуникаций начинали работать строго одновременно и не уходили ни на один такт во время всего сеанса связи. При этом следует сохранить такое качество телефонной связи, как удобство и быстрота вхождения в связь. Это достигается за счет усложнения аппаратуры с применением устройств компьютерного типа.

Основным достоинством систем с цифровым шифрованием является высокая надежность закрытия информации.

Другим преимуществом подобных систем является возможность применения открытого распределения ключей: перед каждым сеансом связи передатчик и приемник автоматически обмениваются открытыми ключами, на основе которых вычисляется секретный сеансовый ключ. Использование этого метода снимает проблему изготовления и рассылки ключей, а также исключает утечку информации из-за недобросовестности в хранении и обращении с ключевыми носителями.

К недостаткам устройств этого класса относятся:

- техническая сложность;
- неустойчивая работа в каналах с большим затуханием;
- низкая степень узнаваемости голоса абонента.

В таблице 2.1 приведены сравнительные характеристики двух принципов закрытия речевого сигнала - аналогового и цифрового.

Таблица 1 - **Сравнительные характеристики аналогового и цифрового принципов закрытия речевого сигнала**

Признак	Принцип закрытия речевого сигнала	
	аналоговый	цифровой
Наличие переговоров в линии телекоммуникаций	есть отчетливые признаки	нет никаких признаков, так как при отсутствии переговоров в линию идет чистый шифр
Распределение амплитуды сигнала	есть ритм и громкость	однородная двоичная последовательность
Остаточная разборчивость	есть признаки начала слова и фразы, паузы	постоянный однородный шум
Кратковременный спектр сигнала	спектральные характеристики неоднородны	однородный

При ведении переговоров работа генератора псевдослучайной последовательности происходит по заданному алгоритму, причем начальная установка для каждого нового разговора вырабатывается и устанавливается в шифраторе заново, при этом в ряде случаев это осуществляется настолько быстро, что собеседники этого просто не замечают. Имеются телефонные шифраторы, которые могут работать с различными линиями телекоммуникаций. Стойкость закрытая информации при этом остается одинаково высокой, а качество речи тем выше, чем шире полоса пропускания канала. Такая универсальность достигается с помощью модемов и дополнительных устройств (рисунок 2.8).

Преимущества цифрового метода шифрования над аналоговым достигаются за счет отказа в большей части случаев от стандартного, телефонного канала и применения сложной и дорогостоящей аппаратуры. В том случае, когда интенсивность переговоров невысока, применение таких устройств экономически неоправданно. Основной характеристикой цифровых шифраторов является применение того или иного криптографического алгоритма. При этом надежность алгоритма считается высокой, если число

ключевых комбинаций более 10^b. Длина ключа у таких устройств порядка 30 знаков, что затрудняет его ввод с клавиатуры,

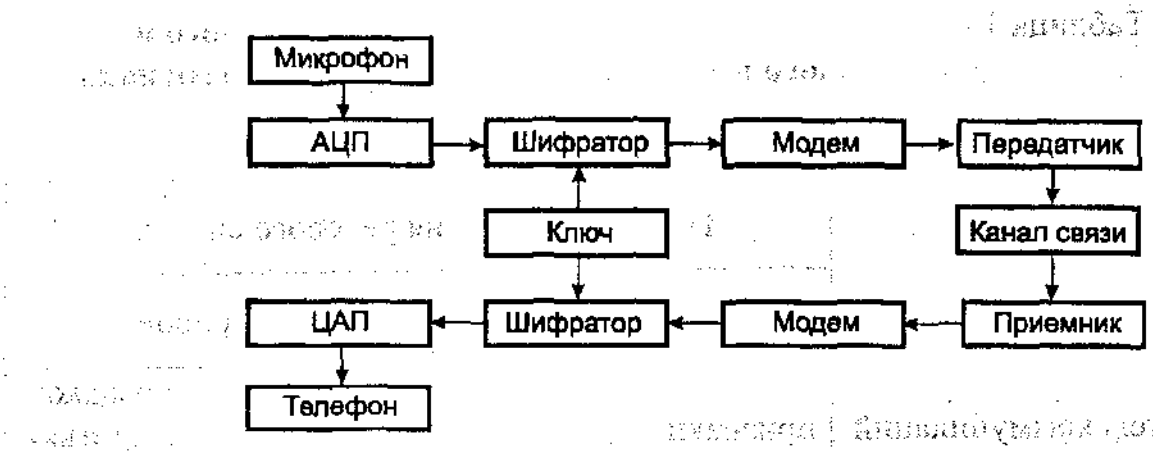


Рисунок 14 - Принцип цифрового метода шифрования

поэтому необходимо обращать внимание на то, в какой форме выполнен ключевой носитель, насколько он надежен и прост в обращении.

Речевые скремблеры типа TRC 769, выпускаемые фирмой Thomson CSF (Франция), защищают телефонные каналы путем частотно-временных перестановок со скользящим окном. Примененный способ временной обработки, в основном, состоит в записи речевою сигнала в память с последующим образованием выборок из сегментов длительностью 32 мс, которые в свою очередь рассеиваются в псевдослучайной последовательности с образованием 14 групп, после чего информация поступает в линию телекоммуникаций. Сигнал объединяется с обратным псевдослучайно распределенным спектром сигнала, который еще больше зашифровывает кодированный сигнал. Амплитуды сегментов речевого сигнала поддерживаются на уровне ниже уровня обычных звуков речи.

Применение такого метода позволяет создать полную неопределенность положения во времени каждого сегмента, повышая тем самым степень закрытости системы. Более того, закон, управляющий временной обработкой речевого сигнала, меняется от сегмента к сегменту неповторяющимся и непредсказуемым способом, поскольку он контролируется сигналами

псевдослучайной последовательности, выдаваемой криптогенератором, то отсутствует необходимость в частом изменении кода системы. В прибор может закладываться одновременно до восьми кодов, что позволяет пользователю связываться с восемью системами телекоммуникаций, каждая из которых может иметь свой собственный (различный) уровень закрытости.

Фирма A-0 Electronics Inc. (США) разработала одноканальный телефон CVAS-III, при работе которого сигнал переводится в цифровую форму, сжимается с помощью PARCOR+LPC алгоритма, шифруется с помощью стандарта DES и передается со скоростью 2410 бит/с. Пользователь не имеет доступа к кодам, вместо этого действует специальный алгоритм выработки секретного кода.

Фирма Grundy and Pathners (Великобритания) разработала полностью автоматический вариант системы зашифровки телефонной связи Model SK. По мнению специалистов фирмы модель, получившая название Cryptophone, может работать в любой общественной или частной телефонной сети, включая использующиеся спутниковые, микроволновые и СВЧ-линии телекоммуникаций. Шифратор Cryptophone использует общее кодовое шифрование (31-элементный цифровой код). Обеспечивается полная безопасность двухпроводной телефонной связи.

Аппаратура серии ANTSEC 2000 фирмы ANT Telecommunication разработана для обеспечения долговременной безопасности речевой связи. Аналоговые сигналы пропускаются через динамический компрессор, сжимаются, а затем с помощью АЦП переводятся в цифровую форму. Преобразование осуществляется с помощью адаптивной дельта-модуляции с частотой синхронизации 64 кГц. После преобразования цифровая информация заносится в память (16 сегментов длиной по 64 мс), образуя одну секцию. Каждый сегмент реорганизуется по времени с помощью микропроцессора и очень сложного алгоритма обеспечивающего максимальное перемещение сегментов в рамках секции. Алгоритм, выбирающий характер реорганизации в рамках каждой новой секции,

контролируется нелинейным кодовым потоком, который, в свою очередь, меняется в соответствии с основным кодом. До использования основного кода для обеспечения закрытия связи в систему вводится часть алгоритма, определяемая пользователем. Основой код состоит из двух частей первая часть ("внутренняя" по отношению к аппаратуре) носит название "серийный код". Количество комбинаций этого кода равно 10^7. Код закладывается в аппаратуру во время производства и редко меняется. Вторая часть кода

находится вне аппаратуры, имеет 10 комбинаций и может быть введена в прибор с помощью простого устройства ввода. Десять выбранных кодов могут одновременно храниться в приборе и меняться по желанию пользователя даже во время работы аппаратуры.

Временная синхронизация в период работы осуществляется каждые 20 сек или 2 мин передачи, в зависимости от требований.

Фирмой Siemens (ФРГ) разработан телефонный аппарат типа Crypset-100, предназначенный для закрытых переговоров. Его особенность состоит в том, что он шифрует и дешифрирует поступающую информацию в автоматическом режиме и передает ее по обычным каналам телефонной связи.

Возможна также работа указанной системы в компьютерном режиме и в режиме Интерфакса. Доступ к аппарату контролируется при помощи электронной охранной системы Smart Card. Каждый пользователь Grypset-100 получает в свое распоряжение опознавательную карточку. Для приведения телефона в рабочее состояние необходимо ввести указанную выше карточку в считывающее устройство, расположенное в корпусе аппарата. Тем самым осуществляется идентификация абонента. В основе этого процесса лежит сличение личного учетного номера (Personal Identification Number) на карточке пользователя с данными оперативного архива. В случае совпадения двух цифровых комбинаций система деблокируется. Далее, путем нажатия на клавишу панели управления телефонного аппарата устанавливается нужный режим его работы -обычный

или закрытый. После этого дешифратор системы по закону случайных чисел выбирает один из 10 вариантов кода и при помощи сигнализатора ставит в известность корреспондента, после чего телефон считается приведенным в рабочее состояние. Далее все происходит обычным путем: набирается нужный номер телефонной сети и следует вызов абонента. Сигнализатор на панели телефона информирует его о предстоящем режиме работы системы. И если он закрытый, то осуществляется описанная выше процедура идентификации личности. Таким образом, становится невозможным перехват информации путем прослушивания телефонного разговора, ведущегося с использованием аппаратуры Grypset-100.

Рассмотрим некоторые зарубежные средства обеспечения безопасности речевой связи.

Фирма Fujitsu (Япония) реализовала DES-алгоритм на двух микропроцессорах, каждый из которых выполняет 16 основных операций. Программа перестановок реализована аппаратно, а замещение выполняется с помощью коммутирующей матрицы с использованием шлюзов NAND. На рисунке 2.9 показана схема шифрования для скремблера с постоянной огибающей спектра. Речевой сигнал делится на 32-мс кадры, которые выбираются в 256 точках с использованием сигнала синхронизации с частотой 8 кГц. В результате операции FFT эти данные из временной области переводятся в частотную разрезанием речевого спектра на 90 частот. Спектр частот в полосе (1,8 - 2,3) кГц, в котором сосредоточивается только небольшая доля энергии речевого сигнала, удаляется и искусственный спектр из 16 частот вставляется на его место. Затем осуществляется перестановка спектра.

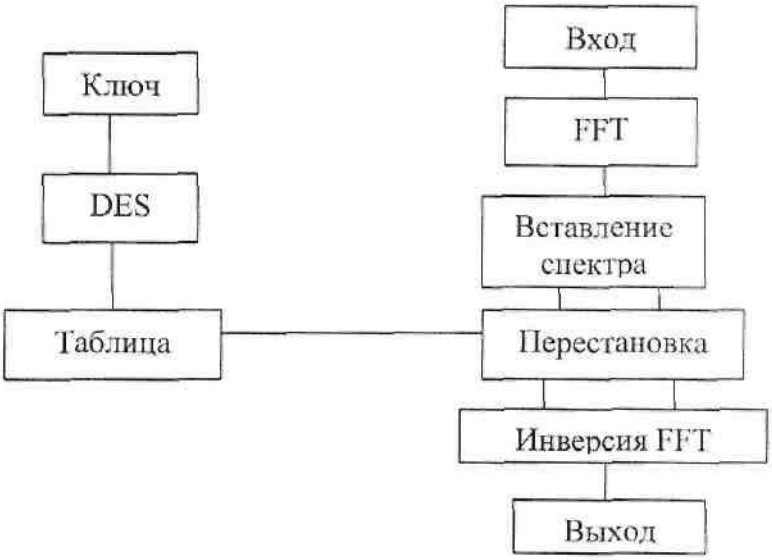


Рисунок 15 - Функциональная схема шифратора уровня огибающей спектра: DES - стандарт шифрования данных; FFT - быстрое преобразование.

Инвертированное FFT-преобразование в результирующем спектре служит для восстановления во временной области и получения зашифрованного выходного сигнала.

Сигнал дешифруется с использованием того же процесса, за исключением того, что искусственный спектр удаляется.

Уровень вставленного искусственного спектра колеблется в зависимости от мощности входного речевого сигнала для регулировки уровня шифрованного выходного сигнала. Когда уровень входного речевого сигнала повышается, уровень вставленного искусственного спектра понижается и наоборот. Это позволяет сохранить постоянный уровень огибающей шифрованного выходного сигнала. Если уровень огибающей возрастает до пикового значения речевого сигнала, то становится субъективно невозможным различить речь и воздействие искусственного сигнала в шифрованном сигнале. Более того, искусственный спектр переставляется совместно с речевым спектром, создавая помехи, что приводит к снижению надежности засекречивания.

Качество сигнала измеряется отношением сигнал-шум SNR (Signal-to-nose Ratio) в сравнении с уровнем входного сигнала.

При значениях SNR 20 дБ и выше обеспечивается удовлетворительная разборчивость речи при дешифровании сигнала. Следует отметить, что при использовании описанного метода необходимо учитывать влияние характеристик канала телекоммуникаций, наиболее важные из которых - групповая задержка сигналов, частота сдвига, прерывание связи.

Рассмотрим систему шифрования речевой связи AVPS. Система AVPS (Analog Voice Privacg System) - это речевой шифратор (скремблер), который осуществляет перестановку отдельных "вырезок" входного сигнала с помощью полосового фильтра-анализатора. Система имеет 12 ключей шифрования, обусловленных возможными перестановками, что обеспечивает надежность используемого метода шифрования для цифровой связи. Система AVPS используется в аппаратуре реального времени и работает с любыми унифицированными телефонами.

Устройство содержит две платы - одну для аналоговой обработки, другую - для цифровой, каждая из них имеет четыре процессора цифровых сигналов.

Системы шифрования речевых сигналов подразделяются на цифровые системы шифрования и аналоговые скремблеры.

Цифровые системы шифрования, как правило, включают три элемента: цифровой кодер, который преобразует речевые сигналы в поток битов, цифровое устройство шифрования и дешифрования, модем (модулятор/демодулятор), который обеспечивает передачу и прием шифрованной цифровой информации по аналоговому телефонному каналу.

В таких системах ограничивающим фактором является то, что модем может реально передавать и принимать только низкоскоростной поток битов, но качество речи от речевых кодеров при таких низких скоростях будет неудовлетворительным. Некоторые низкоскоростные кодеры обеспечивают хорошую разборчивость речи, но при этом страдает естественность речи и не

сохраняются индивидуальные особенности голоса (узнаваемость абонента).

Аналоговые скремблеры позволяют шифровать речь несколькими способами, но не могут передавать ее в виде потока битов. При скремблировании выдается аналоговый сигнал, из которого восстанавливается исходная речь. Основная проблема этого метода засекречивания заключается в том, что простые операции скремблирования, а именно инверсия частоты и временные перестановки, не являются достаточно надежными, что облегчает дешифровку речи.

Системы шифрования с инверсией частоты подобны одноключевым системам. При подслушивании сразу же обнаруживается, что речь шифруется методом инвертирования частоты, поэтому возникает возможность реинвестирования речевого сигнала и расшифровки речи. Метод временных перестановок допускает использование большего числа ключей, но требует существенного увеличения числа уровней обработки для получения разборчивости шифрованной речи. Если временные сегменты речевого импульса выбраны слишком короткими, то в шифрованной речи появляются помехи. Как следствие, аналоговые скремблеры обеспечивают меньшую надежность засекречивания, чем цифровые системы.

Концепция системы. Система шифрования речевых сигналов должна иметь потенциальные возможности для использования большого числа цифровых ключей и обеспечивать высокую надежность засекречивания и в то же время сохранять хорошее качество речи, характерное для лучших аналоговых систем. Система засекречивания должна базироваться на использовании метода частотно-временных перестановок.

Принцип реализации концепции. Речевой сигнал делится на 8 равных частотных полос, и три полосы отбрасываются. Сигнал каждой оставшейся полосы делится на 6 временных сегментов, которые затем переставляются и передаются по каналу. Таким образом, получают 30 возможных вариантов перестановок или 10 возможных ключей. Можно также разделить речевой сигнал на 25 различных временных сегментов для каждой из пяти полос, что

позволяет использовать 125 перестановок или более чем 10 ключей. Хотя число ключей велико, для проверки возможности реализации концепции внесены в ПЗУ-ROM (Real Only Memory) только 10 возможных ключей.

Описываемая система шифрования является полудуплексной, т.е. не может передавать и принимать сигналы одновременно.

Две главные причины для использования полудуплексной системы: она позволяет избежать использования гибридного телефона и эхо-компенсатора, которые необходимы для дуплексной передачи, и требует только четыре цифровых процессора DSP (Digital Processor) - наиболее дорогих компонентов системы. Кроме того, для дуплексной системы требуется двойное число многих цифровых устройств, что приводит к увеличению габаритов аппаратуры шифрования.

Рассмотрим средства обеспечения безопасности речевой информации производства Российской Федерации [13-17].

Маскираторы телефонных разговоров защищают от намеренного, прослушивания или перехвата путем криптографического преобразования на основе личного ключа-пароля абонента. Маскиратор представляет собой малогабаритную приставку к любому типу телефонного аппарата, которая обеспечивает без установки каких-либо специальных устройств на телефонных станциях ведение засекреченных местных и междугородных разговоров. Переход из открытого режима работы в засекреченный и обратно осуществляется нажатием кнопки на маскираторе.

Пользователь может самостоятельно устанавливать кодовую комбинацию на телефонном маскираторе и в процессе разговора увеличивать степень защиты. непосредственно с телефонного аппарата, вводя дополнительный код набором двух или трех цифр. Всего можно использовать более одного млн. возможных цифровых кодов. Маскиратор поддерживает высокое качество речи, что позволяет абонентам узнавать друг друга по голосу.

Маскиратор телефонных разговоров "Туман" выполнен в виде

приставки, располагаемой под телефонным аппаратом и включаемой между ним и микротелефонной трубкой. Принцип его действия основан на аналоговом преобразовании речевого сигнала. При этом невозможно прослушивание телефонного разговора посторонним лицом, не снабженным аналогичным преобразователем.

Основные технические характеристики маскиратора "Туман":

- режим работы ……открытый, защищенный;

- диапазон рабочих частот, кГ…….. 0,3....3,4;

- неравномерность АЧХ сквозного тракта в диапазоне рабочих частот, дБ..... 12;

- коэффициент нелинейных искажений сигнала, %, ……не более 10;

- ток, потребляемый от источника электропитания, …мА, не более 20;

- питание преобразователя от встроенного аккумулятора 7Д-0,115 (батарея "Крона") или от сети переменного тока напряжением, В 220 (50 Гц);

- продолжительность маскированных телефонных разговоров при электропитании от БПС-9/0,3, входящего в комплект маскиратора не ограничена;

- габаритные размеры, мм 200x250x25;

- масса, кг, не более:

а) маскиратора 0,7;

б) БПС-9/0,3..... 0,3.

Другими характеристиками маскираторов могут быть количество кодов (до миллиона), способ ввода ключа (переключатели, номеронабиратель), метод засекречивания, соответствие параметрам сигнала в канале телекоммуникаций, словесная разборчивость восстановленного речевого сигнала, время аппаратной задержки речевого сигнала в тракте передачи-приема.

Абонентский терминал-маскиратор "Исса" позволяет передавать конфиденциальную информацию и данные по телефонным каналам сети общего пользования, а также через УКВ радиостанции, защищая ее от

преднамеренных и случайных искажений знаков и навязывания ложных сообщений. Он обеспечивает:

- первоначальное соединение между абонентами с помощью телефонного аппарата (для носимого варианта - включая телефон-автомат) или микротелефонной гарнитуры радиостанции;
- возможность подключения непосредственно к телефонной линии или радиостанции;
- полудуплексный режим работы по каналу телекоммуникаций со скоростями 1200/600 бит/с;
- передачу сообщения за сеанс объемом до 2560 знаков (один лист формата А4) буквенно-цифрового текста;
- ввод, вывод и редактирование текста;
- хранение набранной информации (при наличии в терминале заряженного аккумулятора) не менее 72ч;
- набор ключа со встроенной клавиатуры.

На базе маскиратора "Уза" могут быть построены локальные системы оперативной конфиденциальной связи.

Устройства передачи конфиденциальной информации предназначены в основном для засекречивания и передачи по телефонному каналу общего пользования конфиденциальных сообщений, представляющих коммерческую тайну. В состав одного такого устройства, например именуемого "Вуаль", входят малогабаритная клавиатура калькуляторного типа, устройство ввода-вывода сообщений и блок питания. Кроме того, оно может быть дополнено устройством документирования сообщений.

Основными характеристиками "Вуали" являются:

- объем буфера текста, знаков:

а) вводимого с клавиатуры…… 75;

б) принимаемого из канала телекоммуникаций…….512;

в) хранимого при отключении питания……..256;

-алфавит открытого текста русские и латинский буквы, цифры,

символы;

-скорость передачи в канале телефонной сети общего пользования, зн./с ……..…….25;

-отображение обработанной информации на жидкокристаллическом индикаторе на 16 знакомест в режиме бегущей строки или построчно;

- длина ключа, знаки 16 или 32;

- одновременное хранение в памяти устройства, ключей до 5;

- гарантированное время пользования ключом без снижения надежности закрытия информации при длине ключа 16 знаков, год ……..1;

-длина пароля, знаки…….....(1.. .8);

-время хранения ключей без замены, мес, не менее ……. 6;

-питание ключевого запоминающего устройства от элементов…РЦ-53У;

-питание устройства от встроенных элементов А3 32 или от сети переменного тока напряжением, В 220 …….…… (50 Гц);

-время непрерывной работы в автономном режиме, ч, не менее..6;

- масса, кг, не более……..

1,5.

В устройстве предусмотрена возможность:

- подключения специализированного печатающего устройства и редактирования информации в процессе ее ввода с клавиатуры;

- защиты от несанкционированного доступа к ключам, хранящимся в памяти устройства, с помощью пароля;

- выработки ключей непосредственно с помощью устройства.

Достоинствами изделия "Вуаль" являются наличие режима формирования ключа, возможность организации сети и индивидуальных связей.

Скремблеры предназначены для защиты телефонных разговоров от несанкционированного прослушивания на линии. Скремблер

аналогоцифровой типа СТА-1000 выполнен в виде малогабаритной подставки под настольный телефонный аппарат любой отечественной и импортной марки, подключается к телефонной сети общего пользования, работает в дуплексном режиме.

Аппаратура засекречивания речи и цифровой информации предназначена для дуплексных, полудуплексных (F-24D) и симплексных (E-24D, E-24) радиоканалов метрового и дециметрового диапазонов, имеющих вход-выход в соответствии с международным стандартом О-И.

Аппаратура обеспечивает засекречивание речи в условиях повышенного уровня шума и цифровой информации, поступающей от источника со скоростью 1200 бит/с, передаваемой по УКВ-ДЦВ радио- или проводным линиям телекоммуникаций.

Речь подвергается дискретизации методом дельта-модуляции со скоростью 16 или 32 кбит/с с последующим позначным шифрованием. Шифрование информации в цифровом виде делает аппаратуру пригодной для работы по телефонным сетям. Ввод ключа может осуществляться с помощью внешнего устройства ввода.

Основные технические характеристики аппаратуры:

- длина ключа, бит..... 128;
- число комбинаций ключа..... $1x10^{38}$;
- число ключевых установок, хранимых в памяти . . . 2;
- время ввода ключа, мин, не более..... 1,5;
- уровень акустического шума, дБ, не более..... . 100;
- время синхронизации, с, не более..... 1,5.

Аппаратура защиты разговоров от подслушивания и звукозаписи гарантирует конфиденциальность при ведении разговоров в любом помещении (квартире, офисе, номере гостиницы и т.п.), не требует специальной подготовки пользователей, является альтернативой дорогостоящим поисковым приборам. Например, с помощью мобильного комплекта защиты от подслушивания G108/P осуществляются постановка

локальной маскирующей помехи и специальная электронная обработка речевых сигналов. При участии в разговоре до четырех человек имеется возможность индивидуальной регулировки громкости, уровень акустической маскирующей помехи не менее 94 дБ. Потребляемая мощность меньше 5 Вт, габаритные размеры 300х20х50 мм, масса 6 кг, время подготовки аппаратуры к работе не более 3 мин.

Аппаратура для ведения конфиденциальных телефонных переговоров АТ-2400. АТ-2400 - это система криптографической защиты телефонных переговоров, использующая преобразование аналогового сигнала в цифровой и его шифрование. Для шифрования используется сложный нелинейный алгоритм, обеспечивающий гарантированную стойкость шифруемых сообщений. Этот алгоритм аттестован к применению для защиты коммерческой информации ФАПСИ (Федеральным агентством правительственной связи и информации при Президенте России).

С помощью аппаратуры АТ-2400 можно сообщать по телефону любую секретную информацию, расшифровать ее без знания ключа невозможно. Ключи к аппаратуре АТ-2400 можно изготавливать самостоятельно на персональном компьютере, возможно использование системы с открытым распределением ключей.

Аппаратура АТ-2400 работает как обычный телефонный аппарат. При необходимости ведения конфиденциальных переговоров нажимается кнопка SEC, переключающая режим работы с открытого на секретный, и через 10-15 секунд после установления синхронизации, на индикаторе появляется надпись "Шифр связь". Это означает, что аппаратура АТ-2400 вошла в режим шифрованной связи и можно вести любые конфиденциальные переговоры. После окончания секретных переговоров можно нажать кнопку CLR, при этом аппаратура АТ-2400 опять будет работать как обычный телефон. При нажатии кнопок SEC и CLR связь с абонентом не прерывается и дополнительных дозвонов не требуется.

Гарантия сохранения конфиденциальности переговоров

обеспечивается в результате того, что:

1. Применяемая для шифрования криптосхема обладает гарантированной стойкостью. Дешифрование практически невозможно без знания ключа.

2. Перед шифрованием аналоговый сигнал преобразуется в цифровой и осуществляется наложение гаммы на цифровой сигнал, что не дает возможности использовать методы бесключевого чтения.

3. В криптосхеме используются специальные методы имитозащиты, не дающие возможности навязать ложное сообщение.

4. Ключ к шифру пользователь имеет возможность выработать самостоятельно.

5. При вскрытии панели устройства ключи стираются.

6. Использованы специальные методы разделения доступа к ключевой системе и защиты от несанкционированного использования аппаратуры.

Технические характеристики аппаратуры АТ-2400:

- управление - клавиши SEC и CLR на панели аппарата и аналогичные клавиши на телефоне;

- дисплей - 16-элементный матричный однострочный ЖКИ;

- основные функции: закрытая телефонная связь, шифрование и передача цифровой информации, функции обычного модема;

- режимы шифрования - речевой сигнал и цифровая информация;

- ввод ключа - из специального устройства;

- долговременный ключ - 10^{100} вариантов, совместим с ключами систем "Анкрипт" и "Криптоцентр";

- разовый ключ - вырабатывается автоматически, количество вариантов превосходит 10 ;

- выработка долговременного ключа - на компьютере с помощью специального программного обеспечения вырабатывается ключ и затем записывается в устройство ввода;

- система с открытым распределением ключей - на компьютере с

помощью специального программного обеспечения вырабатывается общий ключ и записывается в устройство ввода;

- система защиты доступа - независимая система выдачи права ввода ключа в аппарат.

Скремблер "ОРЕХ-А". Для обеспечения конфиденциальных переговоров по телефонным линиям телекоммуникаций разработана криптотелефонная приставка "Орех-А". На основе приставки могут быть построены системы оперативной конфиденциальной телефонной связи.

В криптотелефонной приставке "ОРЕХ-А" закрытие речевой информации достигается следующими методами:

- временных перестановок;

- инверсии спектра сигнала;

- преобразования временного масштаба, разрушающего непрерывность речевого сигнала.

Криптографическая стойкость обеспечивается трехуровневой ключевой системой, включающей в себя:

- ПАРОЛЬ, предназначенный для идентификации абонентов, входящих в связь (вводится с клавиатуры);

- МАСТЕР-КЛЮЧ для заказываемой партии телефонных аппаратов, размещаемый в ППЗУ:

- СЕАНСОВЫЙ КЛЮЧ, генерирующийся физическим датчиком случайных чисел.

Обмен сеансовыми ключами в криптотелефоне реализован по методу открытого распределения ключей с генерацией разовых ключей для каждого сеанса связи (при этом пользователю не требуется вводить ключ в криптотелефон: ключ генерируется самим аппаратом и сохраняется в нем только на время сеанса связи).

Устройство "ОРЕХ-А" обеспечивает:

-защиту от преднамеренного и случайного прослушивания передаваемой речевой информации по телефонным каналам городской и междугородной

телефонной сети, а также от перехвата информации по каналам утечки;

- подключение к телефонным аппаратам, отвечающим требованиям ГОСТ 7153 (Аппараты телефонные общего применения. Общие технические условия);

- полный дуплексный режим;

- словесную разборчивость не менее 90%;

- задержку речевого сигнала в тракте не более 0,32 с;

- подавление скремблированного сигнала на передающей стороне - не менее 30 дБ, подавление сигнала несущей - не менее 40 дБ;

- время установления защищенной связи между двумя абонентами при отношении сигнал/шум 12 дБ - не более 10 с;

-разрядность сеансового ключа -128 бит, разрядность системного ключа -128 бит, разрядность пароля - 4 десятичные цифры (среднее число т/С проб при подборе ключей не менее 10);

- контроль работоспособности в процессе эксплуатации (тест контроля функционирования при включении питания);

- адаптацию к отечественным телефонным линиям телекоммуникаций за счет:

а) подстройки импеданса для согласования с линией;

б) гальванической развязки от телефонной линии и от подключенного аппарата;

-электропитание от сети 220 В 50 Гц, потребляемая мощность приставки - не более 6 ВА.

Конструктивно криптоприставка выполнена в виде подставки под телефонный аппарат с размерами 190х300х40 мм, при этом ее масса не превышает 2 кг. Скремблер "Орех-А" является продуктом научно-технического сотрудничества фирм "АНКАД" и "КРИПТОН", специализирующихся в области защиты данных и речи.

Маскиратор телефонных переговоров TS-001 предназначен для маскировки сообщений в телефонной сети при проведении деловых и

конфиденциальных переговоров между абонентами с использованием ГТС или внутренней сети учреждения.

Основные технические характеристики:

- в состав полукомплекта аппаратуры входит телефонный аппарат типа "Е-086" или "Телур-201" со встроенным устройством аналогового преобразование речевого сигнала. При этом сохраняется возможность работы телефонного аппарата как с преобразованием, так и без преобразования речевого сигнала.

Примечание - Может быть рассмотрена возможность использования телефонных аппаратов других типов.

- полоса передаваемых частот в режиме преобразование - не уже (300-2300) Гц;

- речевая разборчивость преобразованного сигнала при случайном прослушивании на обычный телефон - не более 0,3 %;

- для переключения в режим преобразования речевого сигнала и обратно могут быть использованы как штатные переключатели используемых аппаратов (без сохранения основных функции переключателей), так и установленные специально переключатели.

Для включения аппаратуры в работу следует после соединения абонентов, по взаимной договоренности между ними, перевести переключатель в положение, обеспечивающее маскирование передаваемых сообщений, а по завершении сеанса связи или желании продолжать разговор в обычном (немаскированном) режиме установить переключатель в исходное состояние.

Телефонный аппарат с защитой от прослушивания TS-002 предназначен для зашифрования (скремблирования) и расшифрования речевых сигналов при проведении деловых и конфиденциальных переговоров учреждения.

Зашифрование осуществляется цифровой обработкой временных параметров речевого сигнала. По принципу обработки сигналов TS-002

коренным образом отличается от существующих скремблеров с инверсией спектра и абсолютно не совместим с ними.

Система синхронизации обеспечивает ведение телефонного разговора между абонентами, а том числе и при использовании спутникового канала телекоммуникаций.

TS-002 выполнен в виде телефонного аппарата типа "Телур-201" с памятью последнего набранного номера. Функции телефонного аппарата сохраняются. Путем нажатия специальной кнопки он может быть переведен в обычный режим.

Основные технические характеристики TS-002:

-режим работы псевдодуп-лексный;

-динамический диапазон передаваемых сигналов по сквозному каналу не менее 46 дБ;

-полоса по сквозному каналу не уже 300-3300 Гц;

-разборчивость скремблированного сигнала не менее 0,5%;

-разборчивость и узнаваемость абонента сохраняется полностью;

- задержка передачи информации между абонентами 0,5 с;

- количество комбинаций скремблирования 2 000 000; (конкретная комбинация устанавливается пользователем)

-электропитание от телефонной сети.

3. БЕЗОПАСНОСТЬ ЖИЗНЕДЕЯТЕЛЬНОСТИ

3.1. Влияние метеорологических условий производственной среды на организм человека

Классификация производственного микроклимата и его воздействие на организм.

Производственный микроклимат (метеорологические условия) – климат внутренней среды производственных помещений, определяется действующим на организм человека сочетанием температуры, влажности и скорости движения воздуха, а также температуры окружающих поверхностей.

Производственный микроклимат зависит от климатического пояса и сезона года, характера технологического процесса и вида используемого оборудования, размеров помещений и числа работающих, условий отопления и вентиляции. Однако при всем многообразии микроклиматических условий их можно условно разделить на четыре группы.

1. Микроклимат производственных помещений, в которых технология производства не связана со значительными тепловыделениями. Микроклимат этих помещений в основном зависит от климата, местности, отопления и вентиляции. Здесь возможно лишь незначительное перегревание летом в жаркие дни и охлаждение зимой при недостаточном отоплении.

2. Микроклимат производственных помещений со значительными тепловыделениями. К ним относятся котельные, кузнечные, мартеновские и доменные печи, хлебопекарни, цеха сахарных заводов и др. В горячих цехах большое влияние на микроклимат оказывает тепловое излучение нагретых и раскаленных поверхностей.

3. Микроклимат производственных помещений с искусственным охлаждением воздуха. К ним относятся различные холодильники.

4. Микроклимат открытой атмосферы, зависящий от климатопогодных условий (например, сельскохозяйственные, дорожные и строительные работы).

Одним из важнейших условий нормальной жизнедеятельности человека при выполнении профессиональных функций является сохранение теплового баланса организма при значительных колебаниях различных параметров производственного микроклимата, оказывающего существенное влияние на состояние теплового обмена между человеком и окружающей средой.

Теплообменные функции организма, регулируемые терморегуляторными центрами и корой головного мозга, обеспечивают оптимальное соотношение процессов теплообразования и теплоотдачи в зависимости от конкретных метеорологических условий. Основная роль в теплообменных процессах у человека принадлежит физиологическим механизмам регуляции отдачи тепла.

В обычных климатических условиях теплоотдача осуществляется в основном за счет излучения, примерно 45% всей удаляемой организмом теплоты, конвекции - 30% и испарения - 25%.

При пониженной температуре окружающей среды возрастает удельный вес конвекционно-радиационных теплопотерь. В условиях повышенной температуры среды теплопотери уменьшаются за счет конвекции и излучения, но увеличиваются за счет испарения. При температуре воздуха.ограждений, равной температуре тела, теплоотдача за счет излучения и конвекции практически исчезает и единственным путем теплоотдачи становится испарение пота.

Низкая температура и усиление подвижности воздуха способствуют увеличению теплопотерь конвекцией и испарением.

Роль влажности при пониженных температурах воздуха значительно меньше. В то же время считается, что при низких температурах среды повышенная влажность увеличивает теплопотери организма в результате

интенсивного поглощения водяными парами энергии излучения человека. Однако большое увеличение теплопотерь происходит при непосредственном смачивании поверхности тела и одежды. В производственных условиях, когда температура воздуха и окружающих поверхностей ниже температуры кожи, теплоотдача осуществляется преимущественно конвекцией и излучением. Если температура воздуха и окружающих поверхностей равна температуре кожи или выше ее, теплоотдача происходит за счет испарения влаги с поверхности тела и с верхних дыхательных путей, если воздух не насыщен водяными парами.

Значительная выраженность отдельных факторов микроклимата на производстве может быть причиной физиологических сдвигов в организме рабочих, а в ряде случаев возможно возникновение патологических состояний и профессиональных заболеваний.

Интегральным показателем теплового состояния организма человека является температура тела. О степени напряжения терморегуляторных функций организма и о его тепловом состоянии можно судить также по изменению температуры, кожи и тепловому балансу. Косвенные показатели теплового состояния - влагопотеря и реакция сердечно-сосудистой системы (частота сердечных сокращений, уровень артериального давления и минутный объем крови). Нарушение терморегуляции из-за постоянного перегревания или переохлаждения организма человека вызывает ряд заболеваний.

В условиях избыточной тепловой энергии ограничение или даже полное исключение отдельных путей теплоотдачи может привести к нарушению терморегуляции, в результате которого возможно перегревание организма, т. е. повышение температуры тела, учащение пульса, обильное потоотделение и при сильной степени перегревания - тепловом ударе - расстройство координации движений, адинамия, падение артериального давления, потеря сознания.

Вследствие нарушения водно-солевого баланса может развиться судорожная болезнь, которая проявляется в виде тонических судорог конечностей, слабости, головных болей и др.

При работах на открытом воздухе во время интенсивного прямого облучения головы может произойти солнечный удар, сопровождающийся головной болью, расстройством зрения, рвотой, судорогами, но температура тела остается нормальной.

Воздействие инфракрасного излучения на организм человека вызывает как общие, так и местные реакции. Местная реакция сильнее при облучении длинноволновой радиацией, поэтому при одной и той же интенсивности облучения время переносимости короче, чем при коротковолновой радиации. За счет большой глубины проникновения в ткани тела коротковолновый участок спектра инфракрасной радиации обладает более выраженным общим действием на организм человека.

Под влиянием инфракрасного изучения в организме человека возникают биохимические сдвиги и изменения функционального состояния центральной нервной системы, усиливается секреторная деятельность желудка, поджелудочной и слюнных желез.

Холодовый дискомфорт (конвекционный и радиационный) вызывает в организме человека терморегуляторные сдвиги, направленные на ограничение теплопотерь и увеличение теплообразования. Уменьшение теплопотерь организма происходит за счёт сужения сосудов в периферических тканях.

Под влиянием низких и пониженных температур воздуха могут развиваться ознобления (припухлость, зуд и жжение кожи), обморожения, миозиты, невриты, радикулиты и др. Длительное охлаждение способствует развитию заболеваний периферической нервной, мышечной систем, суставов: радикулитов, невритов, миозитов, ревматоидных заболеваний. При частом и сильном охлаждении конечностей могут иметь место нейротрофические

изменения в тканях.

Нормирование производственного микроклимата и профилактика его неблагоприятного воздействия

Санитарные нормы микроклимата производственных помещений регламентируют нормы производственного микроклимата. В них определена температура воздуха, его относительная влажность, скорость движения воздуха, оптимальные и допустимые величины интенсивности теплового облучения для рабочей зоны с учетом сезона года и тяжести трудовой деятельности.

В производственных помещениях, где невозможно установить допустимые величины микроклимата, необходимо предусматривать мероприятия по защите работающих от возможного перегревания и охлаждения.

Основным путем оздоровления условий труда в горячих цехах является изменение технологического процесса, направленное на ограничение источников тепловыделений и уменьшение времени контакта работающих с нагревающим микроклиматом, а также использование эффективного проветривания, рационализация режима труда и отдыха, питьевого режима, спецодежды.

Наиболее эффективным средством улучшения метеорологических условий является автоматизация и механизация всех процессов, связанных с нагревом изделий.

Значительно уменьшают теплоизлучение и поступление лучистой и конвекционной теплоты в рабочую зону теплоизоляция, отражательные экраны, водяные завесы, вентиляция.

Существенным фактором повышения работоспособности рабочих горячих цехов является соблюдение обоснованного режима труда и отдыха, сокращенный рабочий день, дополнительные перерывы, комнаты отдыха, гидропроцедуры.

Для личной профилактики перегревания существенное значение имеет рациональный питьевой режим. При больших влагопотерях (более 3,5 кг за смену) и значительном времени облучения инфракрасной радиацией - 50% и более - применяется подсоленная (0,3% NaCl) газированная вода с добавлением солей калия и витаминов. При меньших влагопотерях расход солей восполняется пищей. В южных районах страны в горячих цехах применяются белково-витаминный напиток, зеленый байховый чай с добавлением витаминов и др.

В профилактике перегревов большую роль играют средства индивидуальной защиты (спецодежда из хлопчатобумажных, суконных и штапельных тканей, фибровые, дюралевые каски, войлочные шляпы и др.).

Для предупреждения попадания в производственные помещения холодного воздуха необходимо оборудовать у входа воздушные завесы или тамбуры-шлюзы. Если обогрев здания невозможен, применяют воздушное и лучистое отопление. При работе на открытом воздухе в холодных климатических зонах устраивают перерывы на обогрев в специально оборудованных теплых помещениях. Важную роль играет также спецодежда, обувь, рукавицы (из шерсти, меха, искусственных тканей с теплозащитными свойствами, обогреваемая одежда и др.). Прекращение работ на открытом воздухе при низких температурах производится на основании постановления местных органов исполнительной власти.

Регулирование температуры, влажности и чистоты воздуха в помещениях

Необходимые характеристики микроклимата воздуха рабочей зоны, как правило, обеспечиваются вентиляцией.

Под вентиляцией понимают организованный и регулируемый воздухообмен, обеспечивающий удаление из помещения загрязненного воздуха и подачу на его место чистого, определенной влажности и температуры.

Вентиляция бывает естественная и принудительная, общая и местная, организованная и неорганизованная.

Естественная вентиляция осуществляется с помощью проемов в стенах (окон, дверей, фрамуг, форточек) или вентиляционных каналов, без применения специальных механических воздушных насосов (вентиляторов, роторов, компрессоров).

Естественная вентиляция осуществляется аэрационным, дефлекторным или смешанным способами.

Аэрационняа вентиляция осуществляется за счет разности удельного веса холодного и теплого воздуха снаружи и внутри помещения, или напора ветра.

Дефлекторная вентиляция осуществляется за счет разности давлений на концах вентиляционного канала)трубы), которая возникает за счет обдувания скоростным напором ветра одного из концов трубы (как правило, вынесенного на крышу здания).

Чаще всего используют смешанные способы естественной вентиляции, когда используется и разность температур внутри и снаружи помещения и скорость ветра.

Принудительная вентиляция – вентиляция, осуществляемая с помощью механических побудителей (вентиляторов (эжекторов, дефлекторов)) по специальным воздуховодам или каналам.

Принудительная (механическая) вентиляция осуществляется тремя способами. Она бывает вытяжная, приточная и приточно-вытяжная.

При вытяжной вентиляции вентилятором откачивается воздух из помещения. В результате разрежения чистый воздух из окружающей среды или подсобных помещений (через неплотности в окнах, дверях, воздуховодов) поступает внутрь помещения. Применяется, когда загрязнитель воздуха в помещении не является токсичным или пожаровзрывоопасным (избыточное тепло, продукты, дыхания людей или

животных, избыточная влажность).

При приточной вентиляции свежий воздух нагнетается вентилятором в помещение, создавая в нем избыточное давление. При этом загрязненный воздух через окна, двери, воздуховоды выдавливается в окружающую среду. Применяется в случае незначительной концентрации в воздухе вредных веществ, но требуется дополнительная обработка свежего воздуха (подогрев, охлаждение, осушение, увлажнение, ароматизация и т.д.).

Приточно-вытяжная вентиляция предполагает наличие в одном помещении двух вентиляторов, один из которых работает в вытяжном режиме, а другой в приточном. Применяется в случае, когда загрязнитель воздуха токсичен, пожаровзрывоопасен или, когда загрязнитель имеет большую концентрацию в воздухе.

Организованная вентиляция – вентиляция, которая предусмотрена заранее при проектировании здания или рабочего места (двери, форточки, каналы в стенах).

Неорганизованная вентиляция – вентиляция, осуществляемая через неплотности в окнах, дверях, стенах из-за некачественного строительства зданий или неправильной эксплуатации. Этот вид вентиляции не предусмотрен проектом.

Общая вентиляция осуществляется по всему объему помещения или рабочей зоны.

Местная вентиляция осуществляется в зоне ограничесннного объема или рабочего места (над кухонной печью, над столом, химического шкафа).

Для обеспечения необходимых условий труда важное значение имеет кратность воздухообмена, мощность вентиляционных систем и выбор их типа.

Воздухообменом принято называть количество воздуха, которое необходимо подавать в помещение и удалять из него, в кубических метрах за час. Основным показателем является кратность обмена (коэффициент

вентиляции К), которая показывает, сколько раз весь воздух помещения заменяется наружным воздухом в течение часа и рассчитывается по формуле

$$K = \frac{W}{V}, (1/час)$$

где W – объем удаляемого воздуха из помещения, м^3/ч;

V – объем помещения, из которого удаляется воздух, м^3.

Кондиционирование воздуха - это создание и поддержание в закрытых помещениях определенных параметров воздушной среды по температуре, влажности, чистоте, составу, скорости движения и давлению воздуха. Параметры воздушной среды должны быть благоприятными для человека и устойчивыми.

Современные автоматические кондиционерные установки очищают воздух, подогревают или охлаждают его, увлажняют или высушивают в зависимости от времени года и других условий, подвергают ионизации или озонированию, а также подают воздух в помещения с определенной скоростью.

3.2. Пожарная безопасность

Пожар - это горение вне специального очага, которое не контролируется и может привести к массовому поражению и гибели людей, а также к нанесению экологического, материального и другого вреда.

Горение - это химическая реакция окисления, сопровождающаяся выделением теплоты и света. Для возникновения горения требуется наличие трех факторов: горючего вещества, окислителя и источника загорания. Окислителями могут быть кислород, хлор, фтор, бром, йод, окиси азота и другие. Кроме того, необходимо чтобы горючее вещество было нагрето до определенной температуры и находилось в определенном количественном соотношении с окислителем, а источник загорания имел определенную энергию.

Наибольшая скорость горения наблюдается в чистом кислороде. При уменьшении содержания кислорода в воздухе горение прекращается. Горение при достаточной и надмерной концентрации окислителя называется полным, а при его нехватке - неполным.

Выделяют три основных вида самоускорения химической реакции при горении: тепловой, цепной и цепочно-тепловой. Тепловой механизм связан с экзотермичностью процесса окисления и возрастанием скорости химической реакции с повышением температуры. Цепное ускорение реакции связано с катализом превращений, которое осуществляют промежуточные продукты превращений. Реальные процессы горения осуществляются, как правило, по комбинированному (цепочно-тепловой) механизму.

Процесс возникновения горения подразделяется на несколько видов.

Вспышка - быстрое сгорание горючей смеси, не сопровождающееся образованием сжатых газов.

Возгорание - возникновение горения под воздействием источника зажигания.

Воспламенение - возгорание, сопровождающееся появлением пламени.

Самовозгорание - явление резкого увеличения скорости экзотермических реакций, приводящее к возникновению горения вещества при отсутствии источника зажигания.

Самовоспламенение - самовозгорание, сопровождается появлением пламени.

Взрыв - чрезвычайно быстрое (взрывчатое) превращение, сопровождающееся выделением энергии с образованием сжатых газов.

Основными показателями пожарной опасности являются температура самовоспламенения и концентрационные пределы воспламенения.

Температура самовоспламенения характеризует минимальную температуру вещества, при которой происходит резкое увеличение

скорости экзотермических реакций, заканчивающееся возникновением пламенного горения.

Температура вспышки - самая низкая (в условиях специальных испытаний) температура горючего вещества, при которой над поверхностью образуются пары и газы, способные вспыхивать в воздухе от источника зажигания, но скорость их образования еще недостаточна для последующего горения.

Горючими называются вещества, способные самостоятельно гореть после изъятия источника загорания.

По степени горючести вещества делятся на: горючие (сгораемые), трудногорючие (трудносгораемые) и негорючие (несгораемые).

К трудногорючим относятся такие вещества, которые не способны распространять пламя и горят лишь в месте воздействия источника зажигания.

Негорючими являются вещества, не воспламеняющиеся даже при воздействии достаточно мощных источников зажигания (импульсов).

Горючие вещества могут быть в трех агрегатных состояниях: жидком, твердом и газообразном. Большинство горючих веществ независимо от агрегатного состояния при нагревании образует газообразные продукты, которые при смешении с воздухом, содержащим определенное количество кислорода, образуют горючую среду. Горючая среда может образоваться при тонкодисперсном распылении твердых и жидких веществ.

Из горючих газов и пыли образуются горючие смеси при любой температуре, в то время как твердые вещества и жидкости могут образовать горючие смеси только при определенных температурах.

В производственных условиях может иметь место образование смесей горючих газов или паров в любых количественных соотношениях. Однако взрывоопасными эти смеси могут быть только тогда, когда концентрация горючего газа или пара находится между границами воспламеняемых

концентраций.

Минимальная концентрация горючих газов и паров в воздухе, при которой они способны загораться и распространять пламя, называющееся *нижним концентрационным пределом воспламенения* .

Максимальная концентрация горючих газов и паров, при которой еще возможно распространение пламени, называется *верхним концентрационным пределом воспламенения.*

Указанные пределы зависят от температуры газов и паров: при увеличении температуры на 100°С величины нижних пределов воспламенения уменьшаются на 8 -10 %, верхних - увеличиваются на 12 - 15 %.

Пожарная опасность вещества тем больше, чем ниже нижний и выше верхний пределы воспламенения и чем ниже температура самовоспламенения.

Пыли горючих и некоторых не горючих веществ (например алюминий, цинк) могут в смеси с воздухом образовать горючие концентрации.

Наибольшую опасность по взрыву представляет взвешенная в воздухе пыль. Однако и осевшая на конструкциях пыль представляет опасность не только с точки зрения возникновения пожара, но и вторичного взрыва, вызываемого в результате взвихривания пыли при первичном взрыве.

Минимальная концентрация пыли в воздухе, при которой происходит ее загорание, называется *нижним пределом воспламенения пыли* .

Поскольку достижение очень больших концентраций пыли во взвешенном состоянии практически нереально, термин "верхний предел воспламенения" к пылям не применяется.

Воспламенение жидкости может произойти только в том случае, если над ее поверхностью имеется смесь паров с воздухом в определенном количественном соотношении, соответствующим нижнему температурному пределу воспламенения.

Меры по пожарной профилактике.

Мероприятия по пожарной профилактике разделяются на организационные, технические, режимные и эксплуатационные.

Организационные мероприятия: предусматривают правильную эксплуатацию машин и внутризаводского транспорта, правильное содержание зданий, территории, противопожарный инструктаж и тому подобное.

Технические мероприятия: соблюдение противопожарных правил и норм при проектировании зданий, при устройстве электропроводов и оборудования, отопления, вентиляции, освещения, правильное размещение оборудования.

Режимные мероприятия - запрещение курения в неустановленных местах, запрещение сварочных и других огневых работ в пожароопасных помещениях и тому подобное.

Эксплуатационные мероприятия – своевременная профилактика, осмотры, ремонты и практика тушения пожаров наибольшее распространение получили следующие принципы прекращения горения:

изоляция очага горения от воздуха или снижение концентрации кислорода путем разбавления воздуха негорючими газами (углеводы CO $i <$ 12 - 14 %).

охлаждение очага горения ниже определенных температур;

нтенсивное торможение (ингибирование) скорости химической реакции в пламени;

механический срыв пламени струей газа или воды;

создание условий огнепреграждения (условий, когда пламя распространяется через узкие каналы).

ЗАКЛЮЧЕНИЕ

На основании проведенных по данному этапу НИР исследований можно сделать нижеследующие выводы.

1.Как показывает международная практика в целях защиты обмена информацией между двумя пользователями используют два пути. Первый - подключение к защищенной государственной системе телекоммуникаций, второй - организация обмена информацией по сетям телекоммуникаций общего пользования, например, ТфОП.

2.Одним из вопросов, возникающих на широко используемом втором пути, является оценка доступности для злоумышленника используемых телефонных линий и коммутационных узлов сети. Анализ показывает, что ТфОП имеет недостаточный уровень защиты линий и коммутационного оборудования.

3.Отсутствие достаточного уровня защиты ТфОП во многом связано с тем, что существующая правовая база не дает достаточной основы для защиты информации, поэтому коммутируемая телефонная сеть общего пользования без использования специальных мероприятий, методов и средств не может гарантировать защиту информации.

4.Отсутствие контроля за состоянием отдельных компонентов абонентских линий (АЛ) и специальных средств защиты позволяет злоумышленникам осуществлять свою противоправную деятельность. В связи с этим операторы ТфОП должны ясно осознавать угрозы безопасному функционированию своих сетей, если не будут приняты оперативные меры по обеспечению защиты и предотвращения действий злоумышленников.

5.Исследования показывают, что в ТфОП наиболее уязвимым сегментом, подверженным воздействию злоумышленников, является абонентская линия, поэтому вопросы защиты информации в АЛ приобретают в последнее время особенное значение.

6.Качественная защита АЛ должна охватывать все основные

направления защиты информации и должна обеспечиваться комплексом правовых, организационных и режимных мероприятий, а также технических мер и средств с учетом развития ТфОП

7.В данном промежуточном отчете рассмотрены основные принципы и способы несанкционированного доступа (подключений) различных злоумышленников к АЛ, а также меры по защите информации.

8.Проведенный анализ показал, что методы защиты от утечки информации подразделяются на организационные или организационно-технические, аппаратные или программно-аппаратные.

9.Простейшими устройствами обнаружения несанкционированных подключений (НСП) к АЛ являются разнообразные индикаторы состояния, которые осуществляют контроль за изменениями параметров АЛ. Для проведения углубленных исследований АЛ и локализации места НСП используются анализаторы телефонных линий и кабельные радары.

10.Кроме вышеописанных способов широкое применение на практике нашли методы и технические средства с использованием зачумляющего воздействия на АЛ. Необходимо, однако, отметить, что вышерассмотренные методы и средства обеспечивают недостаточно высокую степень защиты АЛ от НСД, которая зависит от возможностей потенциального злоумышленника по технической реализации способа преодоления механизма защиты.

10 В отличие от вышерассмотренных устройств, более эффективными по степени обеспечиваемой защиты являются средства криптографической защиты информации: маскираторы, скремблеры и шифраторы, которые реализуют разнообразные принципы преобразования передаваемого сигнала.

Список использованных источников

1. Дубровский Е.П. Абонентские устройства городских телефонных сетей. / Справочник. - М.: Радио и связь, 1986

2. Разработка методов защиты абонентских линий сетей телекоммуникаций от НСД к международным и междугородным услугам телекоммуникаций. Отчет о НИР. - Т.: ЦНТМИ, 2000.

3. Минаев В.А., Скрыль СВ. и др. Безопасность информационно-телекоммуникационных систем: основные тенденции развития // Системы безопасности связи и телекоммуникаций, 2001, июнь-июль, с. 74-77

4. Воронин В.С., Первоочередные проблемы обеспечения безопасности информационных сетей связи. // Автоматика, связь, информатика, № 7, 2001, с. 12-13

5. Годный В.Г., Мансуров В.В. Информационная безопасность сетей связи на базе УПАТС. // Системы безопасности связи и телекоммуникаций, 2002, июнь-июль, с. 74-77

6. Сенашенко Д., Коровин И. Вопросы безопасности цифровых АТС зарубежного и российского производства. // Безопасность, достоверность, информация (БДИ), 2001, № 6, с. 38-40.

7. Сенашенко Д. Вопросы безопасности цифровых АТС зарубежного и российского производства. // Безопасность, достоверность, информация (БДИ), 2002, №2, с. 58-61.

8. Поташов А.И. Законодательные основы приобретения и эксплуатации автоматических телефонных станций. // Системы безопасности связи и телекоммуникаций, 2001 декабрь, с 50-54

9. Савлуков Н.В. Проблемы информационной безопасности телекоммуникационной компании АО МГТС // Доклад на международной конференции "Телекоммуникации в аспекте национальной безопасности. Перспективы развития информационно-телекоммуникационной структуры" - С.-Пб., ноябрь, 1998

10. Голубев А.Н., Гольдштейн Б.С, Гончарок М.Х. Основные принципы

построения системы защиты информации в узлах коммутации // Электросвязь, №1, 2002.

П.Кравченко В.Б. Защита речевой информации в каналах связи. - http:/www.bezpeka.com

12. Попов Ю.Г. Некоторые вопросы защиты информации в цифровых АТС. Ежегодный отраслевой каталог. // Техника и средства связи, 1998, с. 183-184

13. И.Барсуков В.С. Обеспечение информационной безопасности. / Справочное пособие - М.: Экотрендз, 1996

14. Н.Петраков А.В., Лагутин В.С. Утечка и защита информации в телефонных каналах. - М.: Энергоатомиздат, 1997

15.Иванова Т.И. Абонентские терминалы и компьютерная телефония. - М.: Экотрендз, 1999

16.Хорев А.А. Способы и средства защиты информации. - М.: МОРФ, 1998

17. Организация и современные методы защиты информации. Под общ. ред. Диева С.А. и др. - М.: Концерн Банковский деловой центр, 1998.

18. http://aktrb.by/products/obnaruzhenie-vzryivnyih-ustroystv