А.Фантомэ
инженер, техническая защита информации.

Кишинёв
2020

ТЕХНИЧЕСКИЕ КАНАЛЫ УТЕЧКИ ИНФОРМАЦИИ, ПЕРЕДАВАЕМОЙ ПО КАНАЛАМ СВЯЗИ.

О том, что его телефон – и в прокуратуре и дома – прослушивается, Берг не подумал. Он считал, что это может быть сделано лишь с санкции отдела юстиции западноберлинского сената, который – Берг был убеждён – сейчас на это не пойдёт.

Он недоучёл лишь того, что телефонная сеть города обслуживалась двумя компаниями, в одной из которых концерн Дорнброка обладал контрольным пакетом акций. (“Все революции, – говорил Дорнброк, – проваливались или побеждали в зависимости от того, удавалось ли бунтовщикам овладеть средствами связи”.)

Юлиан Семёнов, “Бомба для председателя”

Небольшое вступление.

Данная презентация создавалась как “наглядное пособие” для проведения занятий по вопросам, связанным с утечкой информации, передаваемой по каналам связи.
При этом в ней **рассматриваются угрозы, связанные именно с телефонными переговорами** (*в том числе, ведущимся по сетям ISDN и VoIP*).
Варианты угроз, касающиеся “полноценного” мониторинга сетей передачи данных, в данной презентации не рассматриваются.

Основными слушателями, для которых делалась данная презентация, были не “технари” в области ТЗИ, а сотрудники подразделений информационных технологий, служб безопасности и личной охраны – *в той или иной мере сталкивающиеся с данной проблемой*.

Основная цель занятий была показать, что существуют различные способы съёма информации, циркулирующей в телефонных сетях.
Кроме того, хотелось по возможности развеять “фильмово-фантастическое” представление в этой области, которое к сожалению присутствует – *причём, очень крепко присутствует* – у многих граждан.

Небольшое вступление.

Данная презентация рассчитана на “коммерческо-частный сектор”:
в ней рассматриваются средства и системы связи, повседневно используемые “обычными” пользователями и угрозы, которые могут быть реализованы в их отношении.
При этом предполагается, что потенциальный злоумышленник так же является представителем “коммерческого-частного сектора” и может обладать соответствующими возможностями (*как материально-финансовыми, так и “административными”*) – пусть “достаточно большими”, в ряде случаев – незаконными, но всё равно “ограниченными”.

Варианты, связанные с “силовыми структурами” – когда задействуются “возможности государства” – это совсем другое дело.
Некоторые примеры “возможностей государства” в этой области приведены на слайдах “Примеры из истории”.

Что касается “отношений обычных граждан и государства”, то как говорится:
“**Если вами заинтересовалось государство – считайте, что вам не повезло**”.
Поэтому нужно не нарушать закон и не давать повода к тому, чтобы “государство вами заинтересовалось”.

Небольшое вступление.

Как и в предыдущих презентациях, в “презентационный вариант” были переведены схемы, рисунки и таблицы из учебного пособия А.А.Хорева (*Хорев А.А. Техническая защита информации. Т.1. Технические каналы утечки информации. – М.: ООО “НПЦ Аналитика”, 2008)* – в основном это касается угроз, актуальных для “классической” и беспроводной телефонии. Угрозы, связанные с перехватом телефонных переговоров, передаваемых с помощью ВОЛС, представлены на основе учебного курса *В.В.Гришачева “Информационная безопасность волоконно-оптических технологий”*.

Кроме того, в презентации рассматриваются некоторые моменты, связанные с утечкой информации за счёт “дополнительных функций” и “неграмотного использования” типовых телекоммуникационных систем, а так же за счёт “естественных каналов утечки”.

Вопросы, связанные с утечкой акустической информации из помещений, в которых установлены средства связи: *“микрофонный эффект”, “ВЧ-навязывание”, передача “акустики” по телефонной линии, съём “акустики” за счёт “дополнительных” или “не декларированных” возможностей телекоммуникационного оборудования и т.д*. – в данной презентации не рассматриваются – все эти моменты обсуждаются в презентации “**Технические каналы утечки акустической информации**”.

Небольшое вступление.

Структурно презентация состоит из двух “составляющих”:
в первой рассматриваются принципы построения той или иной системы связи,
во второй речь идёт уже непосредственно о возможных угрозах.

Текста в презентации мало – в каждом конкретном случае он читается “из головы” в зависимости от подготовленности и “специфики” аудитории.

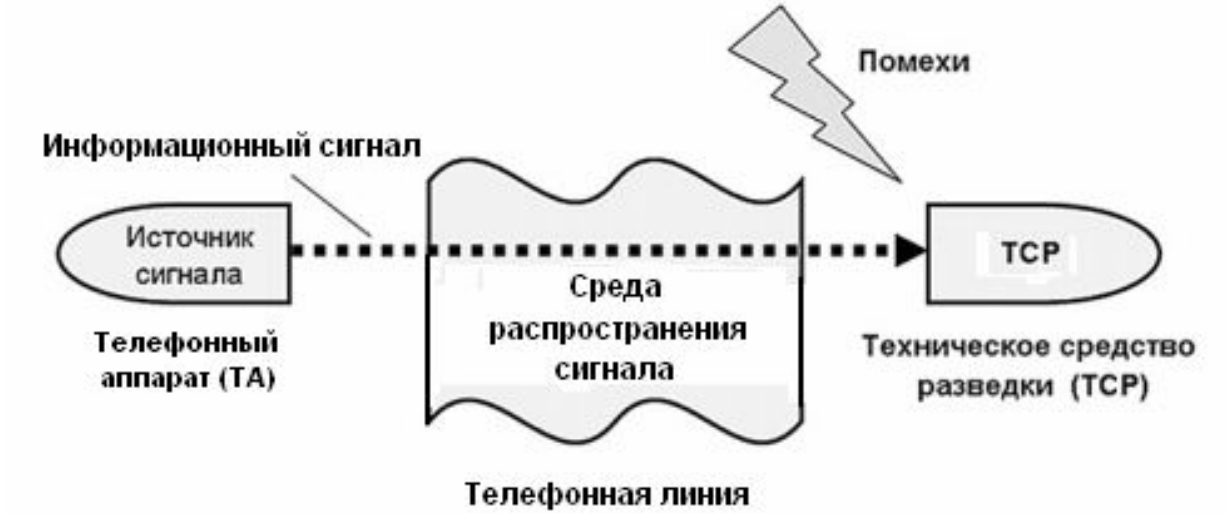
Перед просмотром данной презентации настоятельно советую прочитать мои “замечания” к ней в соответствующем разделе форума на сайте www.analitika.info – это сразу снимет ряд возможных вопросов.

Схема канала утечки информации.

Под **техническим каналом утечки информации (ТКУИ)** понимают совокупность объекта разведки (*технического средства обработки и передачи информации*), технического средства разведки (**ТСР**), с помощью которого перехватывается информация, и физической среды, в которой распространяется информационный сигнал.

Типовая схема телефонного канала передачи информации.

Схема канала утечки информации, передаваемой по телефонной линии.

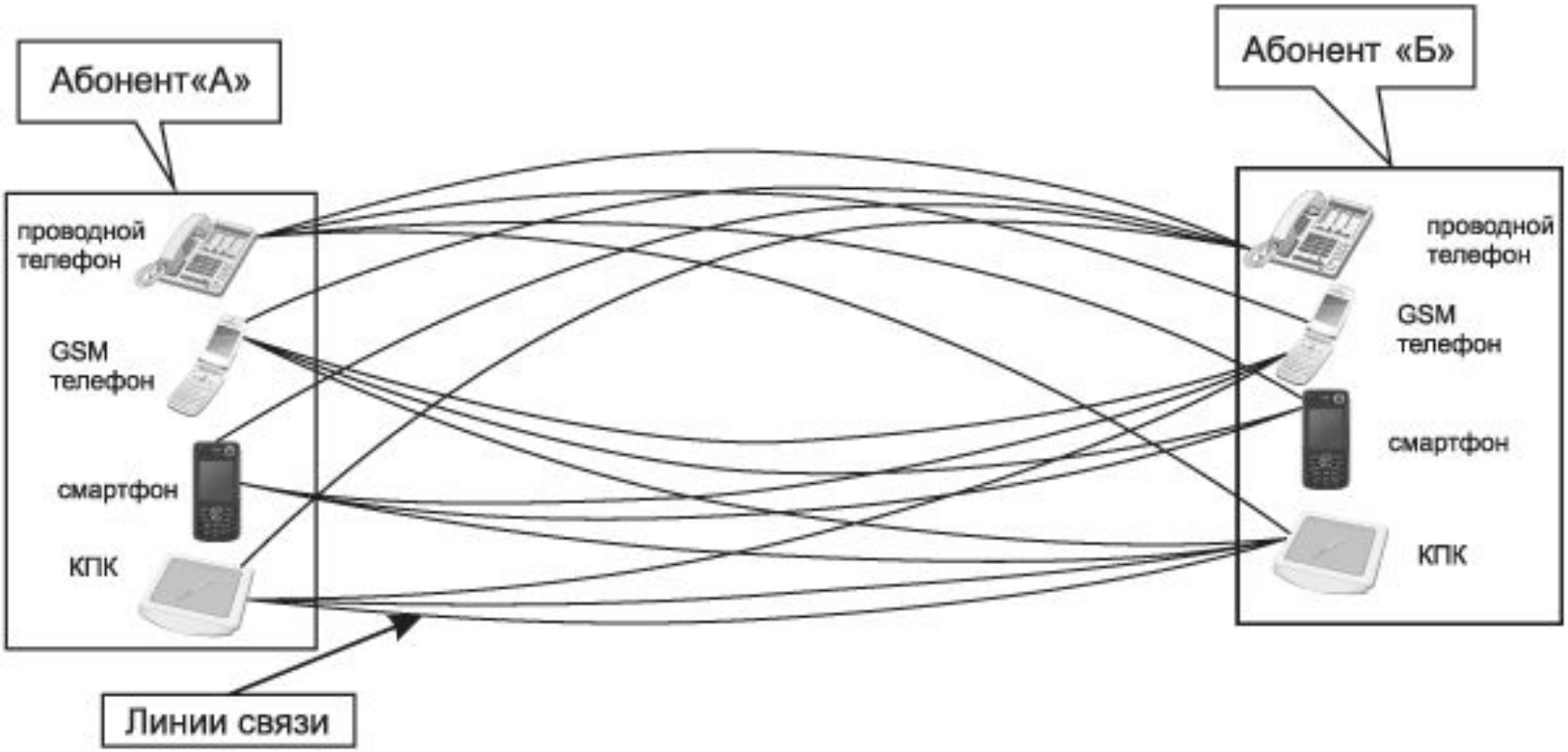


Хорев А.А. “Технические каналы утечки информации, передаваемой по каналам связи” / “Специальная техника”, 2004 г. № 6.

“Классическая” модель связи (*для двух абонентов*).

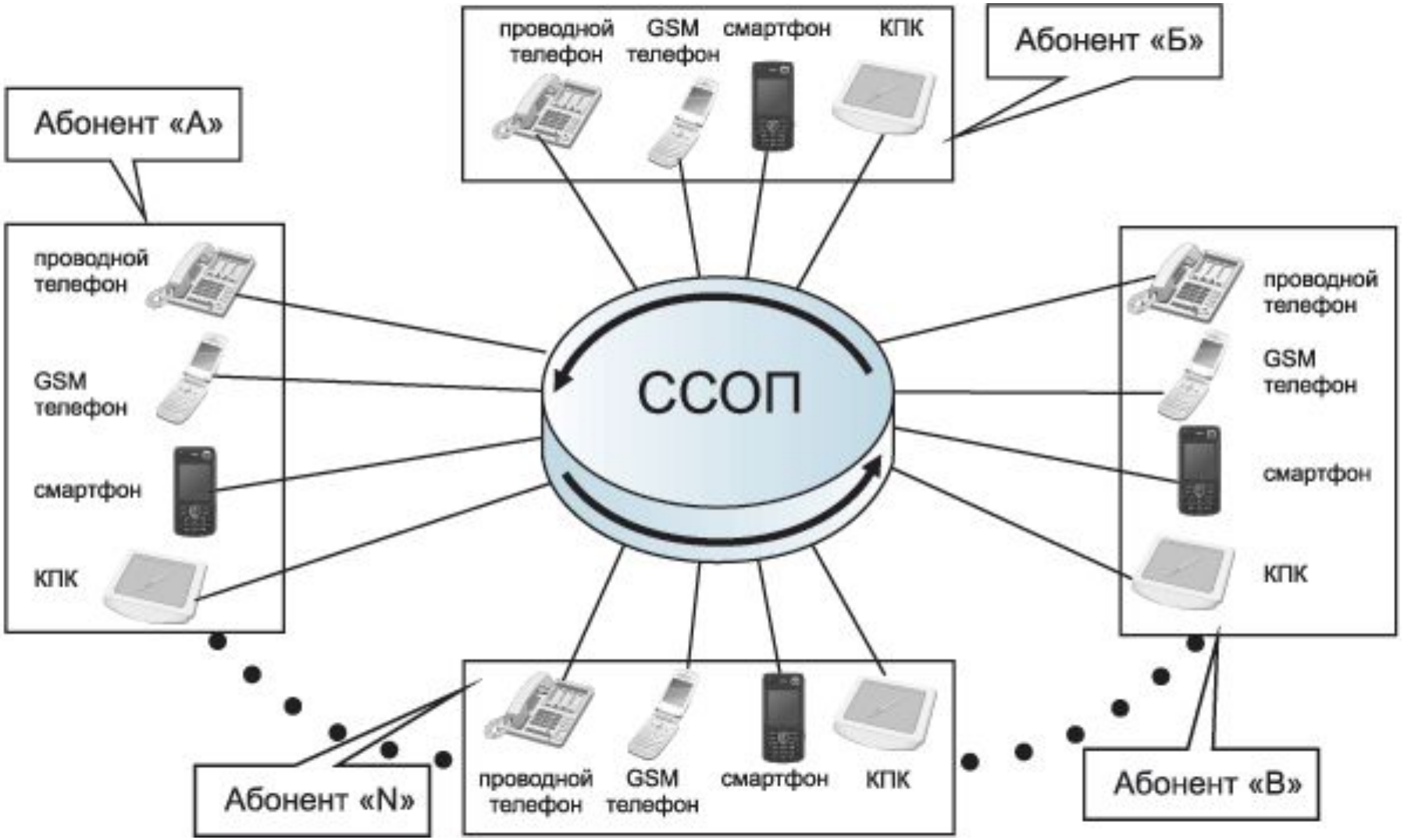
Данная модель характерна для стационарных абонентов: оба абонента подключены к одной сети через стандартные проводные окончания, принадлежащие непосредственно данным абонентам.

“Современная” модель связи (*для двух абонентов*).



Данная модель характерна для случаев, когда хотя бы один абонент подвижен (*в роли абонентского терминала выступает беспроводное устройство, не имеющее стандартного проводного стыка*) или когда хотя бы один абонент находится в “блуждающем” режиме – т.е. входит в сеть через “случайные” абонентские терминалы (*“разовые” мобильные телефоны, телефоны в местах случайного посещения, таксофоны и т.п.*).

“Современная” модель связи (*для большого числа абонентов*).



Классификация технических каналов утечки информации, передаваемой по каналам связи.

Классификация технических каналов утечки информации, передаваемой по каналам связи, имеет многоуровневый характер – это определяется наличием целого ряда факторов, связанных с их возникновением и функционированием.

Например, ТКУИ могут быть классифицированы:

- По происхождению: **искусственные** (*преднамеренно созданные злоумышленником*) и **естественные**.
- По степени функционирования: **реально действующие** и **потенциально возможные** (*не используемые в данный момент злоумышленником*).
- По физической природе образования: **электромагнитные**, **электрические**, **индукционные** и т.д.
- По методу ведения разведки: на базе средств **пассивного перехвата** и на базе средств **активного перехвата**.
- По технологии (*тактике*) применения технических средств разведки: с использованием **вносимых *(заносных)* ТСР**, с использованием **заранее внедряемых ТСР**, с использованием **“беззаходовых” ТСР**.

Можно привести и другие варианты классификации технических каналов утечки информации, в основу которых положены свои “критерии отбора”, но при этом “высший смысл” всех этих классификаций остаётся, в принципе, одним и тем же и позволяет охватить все возможные варианты угроз.

Вариант классификации технических каналов утечки информации, передаваемой по каналам связи.

Определение СТС.

Постановлением Правительства РМ № 100 от 9 февраля 2009 г. дано определение **специальных технических средств**, предназначенных для негласного получения информации: технические и/или программные средства, разработанные, приспособленные или запрограммированные для съёма, получения, перехвата, сбора, прослушивания, регистрации и передачи акустических, видовых, электромагнитных и других сигналов с целью получения негласного доступа к информации, в том числе циркулирующей в сетях электронных коммуникаций.

В соответствии с **Классификатором специальных технических средств, предназначенных для негласного получения информации** (Приложение № 2 к Постановлению Правительства РМ № 100 от 09.02.2009) определён перечень **Специальных технических средств (СТС), предназначенных для негласного прослушивания телефонных переговоров и перехвата информации, циркулирующей в сетях электронных коммуникаций** (п. 3 и п. 4 “Классификатора…”).

СТС или не СТС – вот в чём вопрос...

Согласно действующего законодательства “оборот” СТС строго ограничен, а право на их использование имеют только государственные структуры, являющиеся субъектами оперативно-розыскной деятельности.
Однако **существующие реалии таковы**, что определённые типы СТС могут быть изготовлены или “относительно свободно” приобретены не только“силовиками”.
Как результат – использование СТС на сегодняшний день возможно “не только в государственных интересах”.

В то же время, **необходимо чётко понимать**, что во многих случаях утечка и съём информации, передаваемой по каналам связи, могут быть реализованы и без использования СТС.
Существует множество устройств и систем “бытового назначения”, которые случайно или преднамеренно могут быть использованы для этих целей: начиная “параллельным телефоном” или “трубкой монтёра” и заканчивая различными “аппаратно-программными вариантами”, которые **штатно предусмотрены** во многих современных системах связи: конференцсвязь, “вклинивание в разговор”, запись разговора в “систему голосовой почты” и т.д.

Системы стационарной телефонной связи.

В настоящее время “стационарная” телефонная связь продолжает активно развиваться и активно использоваться “теми, кто понимает и кому это нужно” – не смотря на тот факт, что некоторая часть населения уже полностью ушла в “мобильно-планшетный мир” и почти забыла, что есть “обычный” телефон, письма в конвертах и бумажные книги в переплёте.

Современная стационарная телефония обладает большими возможностями и предоставляет широкий спектр услуг, которые востребованы как частными лицами, так и коммерческими структурами.

Для многих “обычных” пользователей телефонная связь ассоциируется только с телефонным аппаратом (*пусть даже и “навороченным”*), стоящим на столе.

На самом деле в техническом плане там всё намного сложнее.

Системы стационарной телефонной связи.

Можно условно выделить несколько схем построения стационарной телефонной связи: **“классическая”** – *городская АТС находится “где-то там” и от неё до абонентов проложены абонентские кабели, а на “своей территории” находится только телефонный аппарат и часть абонентской линии*, **“классическая на базе собственной мини-АТС”** – *как правило, практически всё оборудование находится на “своей территории” (если только к АТС не подключены “внешние” линии)*, **“современные”** варианты на основе технологий типа ISDN и VoIP.

В качестве примера более подробно рассмотрим “классические” варианты стационарной телефонной связи.

Исходя из особенностей построения “классических” стационарных телефонных станций их оборудование можно разделить на три группы: станционное, линейно-кабельное и оконечные абонентские устройства.

Системы стационарной телефонной связи.

Станционное оборудование включает в себя:

- Непосредственно автоматические телефонные станции (АТС).
- Устройства коммутации цепей станционного монтажа (*кроссы и т.п.*).
- Кабели станционного монтажа.
- Другое оборудование станции, предусмотренное техническим проектом.

Линейно-кабельное оборудование включает в себя:

- Распределительные устройства (*распределительные шкафы и коробки, кабельные боксы*).
- Магистральные абонентские кабели, соединяющие абонентский кросс с распределительными устройствами.
- Распределительные абонентские кабели, соединяющие оконечные распределительные коробки с абонентским кроссом или с распределительными шкафами.
- Абонентскую проводку, соединяющую оконечные распределительные коробки с оконечными абонентскими устройствами.

Оконечные абонентские устройства включают в себя телефонные аппараты и другие устройства, допущенные к эксплуатации в сети связи.

Системы стационарной телефонной связи.

Перехват информации может быть осуществлён на любом из вышеуказанных участков, но для каждого из них имеются свои наиболее вероятные виды угроз.

При этом нужно чётко понимать, что для подключения (*установки*) средств съёма информации злоумышленнику необходим физический доступ к оборудованию телефонной сети (*хотя бы на короткое время*).

В ряде случаев возможны некоторые “беззаходовые” варианты – *типа т.н. “Fly-подключений” или с использованием “дополнительных функций” АТС* – но тут тоже не всё так просто: нужно как минимум быть “абонентом данной сети”.

Наиболее идеальный (*с точки зрения злоумышленника*) вариант – это доступ к станционному оборудованию (непосредственно к АТС или к абонентскому кроссу). В этом случае можно без проблем (*с технической точки зрения*) контролировать любого абонента данной сети.

Но на практике в большинстве случаев “постороннему человеку” получить такой доступ практически невозможно. И если у злоумышленника нет “своих людей” на АТС (*причём тех, кто может “реально решать вопросы”*), то этот вариант отпадает.

Примечание: *в качестве злоумышленника рассматриваются представители “коммерческо-частного сектора” с соответствующими возможностями*.

Системы стационарной телефонной связи.

Как правило, наиболее доступный для злоумышленника вариант – это подключение к линейно-кабельному оборудованию или непосредственно к оконечным абонентским устройствам.

В частности, речь идёт о распределительных устройствах: шкафах, коробках, кабельных боксах и т.п.

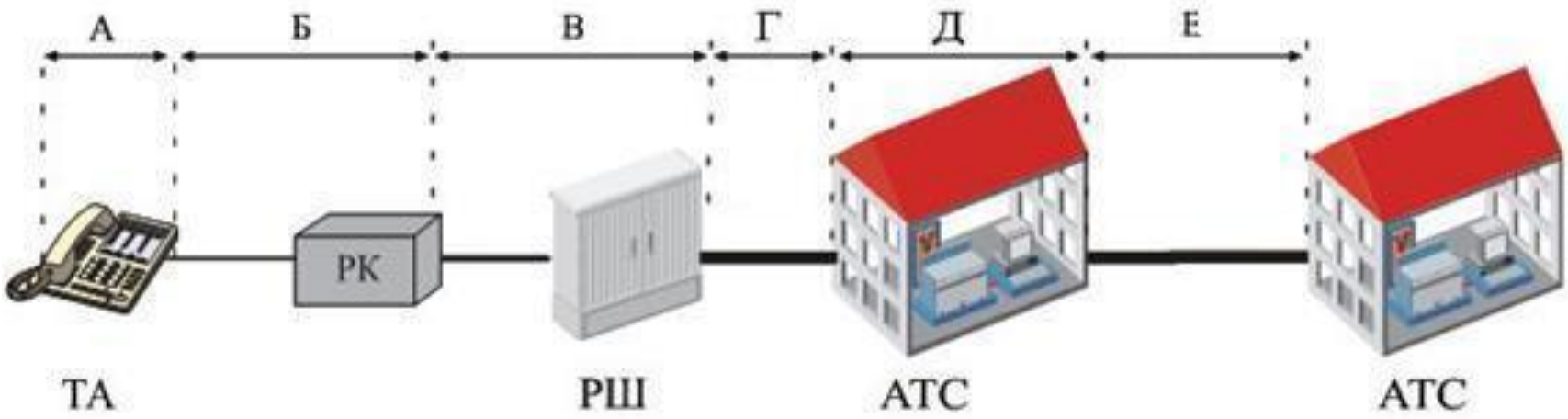
Очень часто это оборудование размещается в “относительно бесконтрольных” местах (*в подвалах, на чердаках, в каких-то подсобных помещениях и т.п.*), где возможен свободный доступ к нему – всё определяется “степенью бардака”.

Кроме того, контроль данного оборудования обслуживающим техперсоналом осуществляется достаточно редко (*обычно в случае какой-либо “аварии” или при подключении “нового абонента”*) – поэтому вероятность обнаружения каких-либо действий злоумышленника достаточно низка.

Аналогичная ситуация и с распределительными кабелями: если кабель проложен где-то в подвале или на чердаке, то периодичность его осмотра техперсоналом “стремится к бесконечности” – *пока его не перегрызут крысы или пока бомжи не вырежут его на цветной металл*.

Примечание: *в качестве злоумышленника рассматриваются представители “коммерческо-частного сектора” с соответствующими возможностями*.

Обобщённая структура городской телефонной сети.



Типовая “классическая” абонентская телефонная линия состоит из пары проводов, проложенных от телефонной розетки до распределительной коробки (РК) – ***абонентский участок***. Далее она идёт по многопарному кабелю до распределительного шкафа (РШ) – ***распределительный участок***, а затем – по многопарному бронированному кабелю до АТС – ***магистральный участок***.

Между АТС прокладываются симметричные или коаксиальные высокочастотные кабели. В то же время, учитывая “цифровизацию” телекоммуникационных систем, на ряде участков сигнал может передаваться не в аналоговой, а в цифровой форме с использованием ВОЛС (*соединения между АТС, соединение от АТС до РШ*).

А в ряде случаев “цифровое окончание” может подаваться непосредственно к абоненту (*в виде оптоволокна или “витой пары”*).

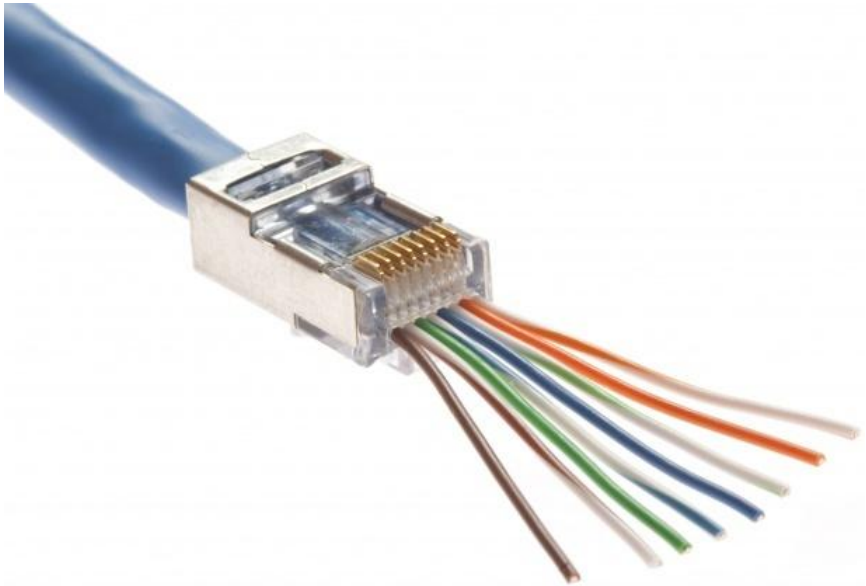
Примеры оконечных абонентских устройств.

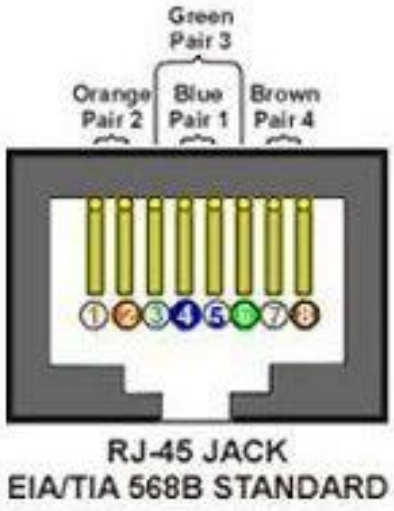
Примеры оконечных абонентских устройств.

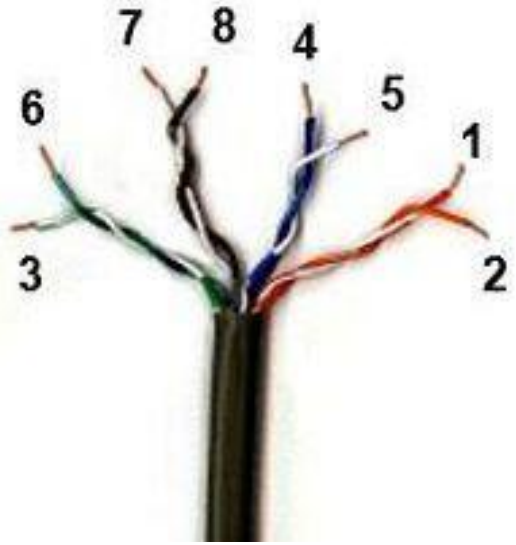
Примеры оконечных абонентских устройств.

Примеры кабелей (проводов), используемых для подключения телефонного аппарата (разъём RJ-11).

Типовой разъём RJ-45.

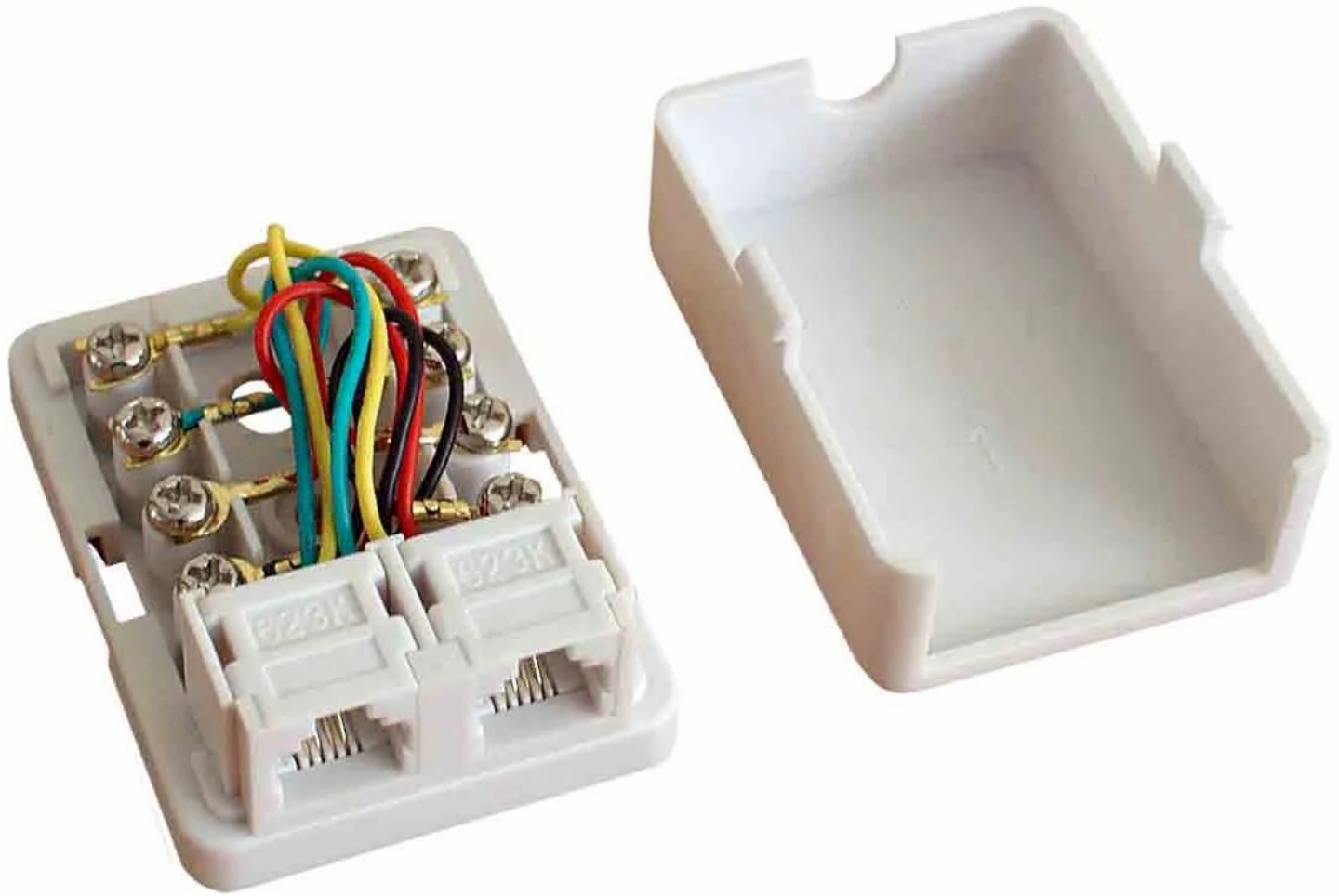




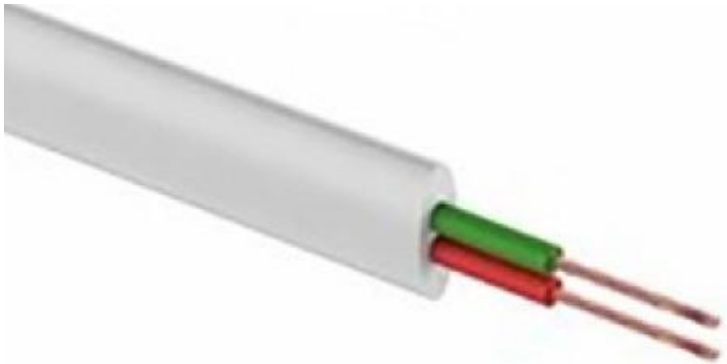


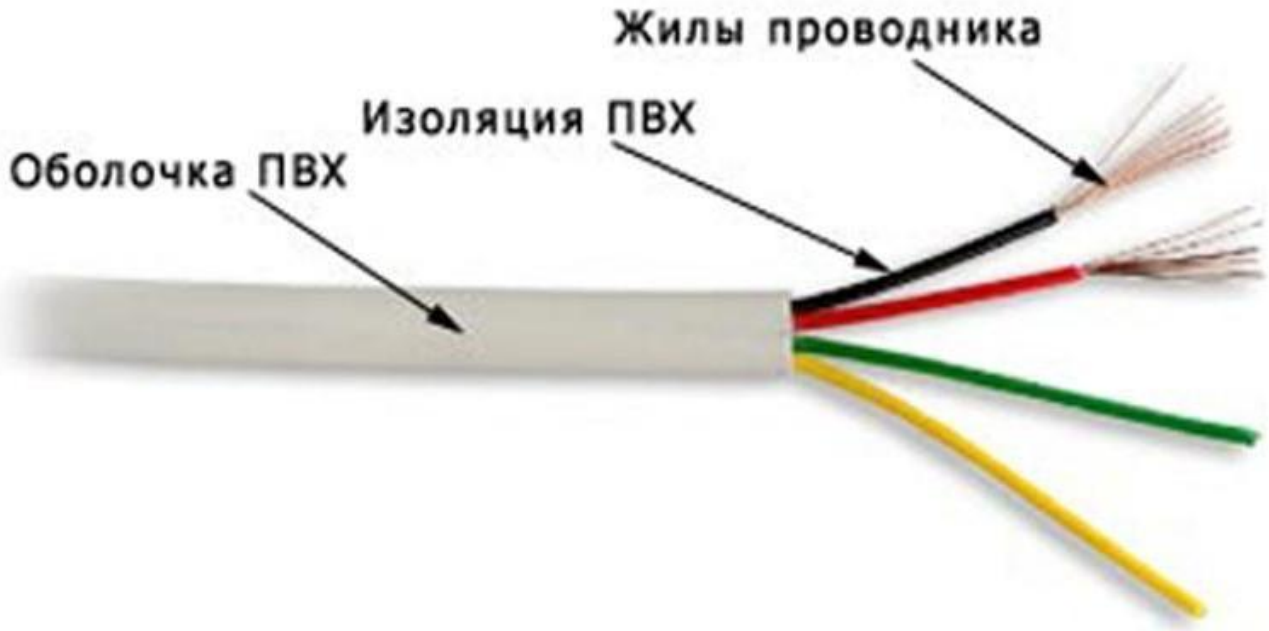
Варианты телефонных розеток.

Типовая телефонная розетка (“евро”).

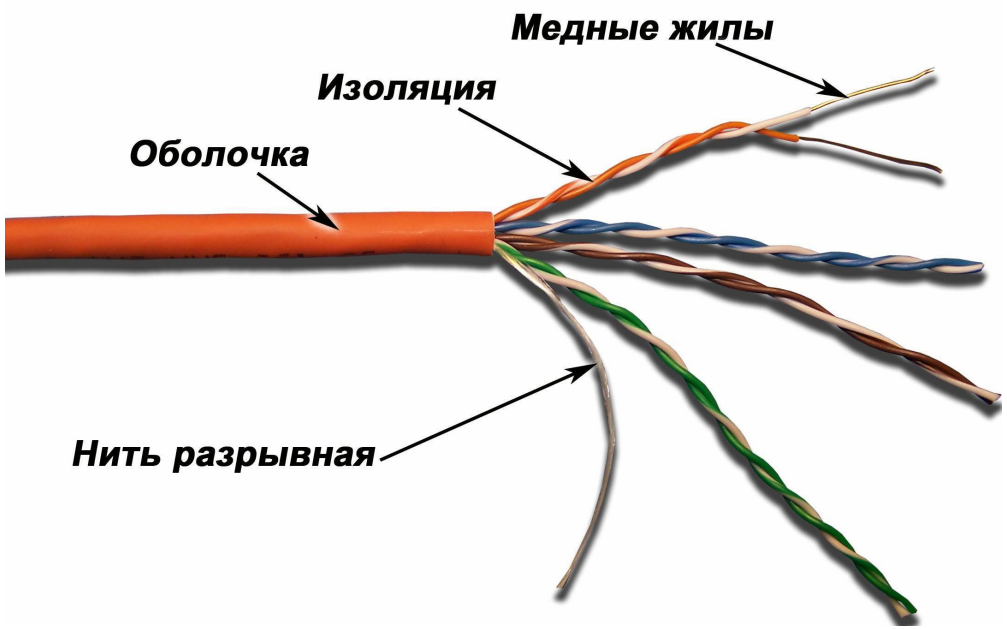


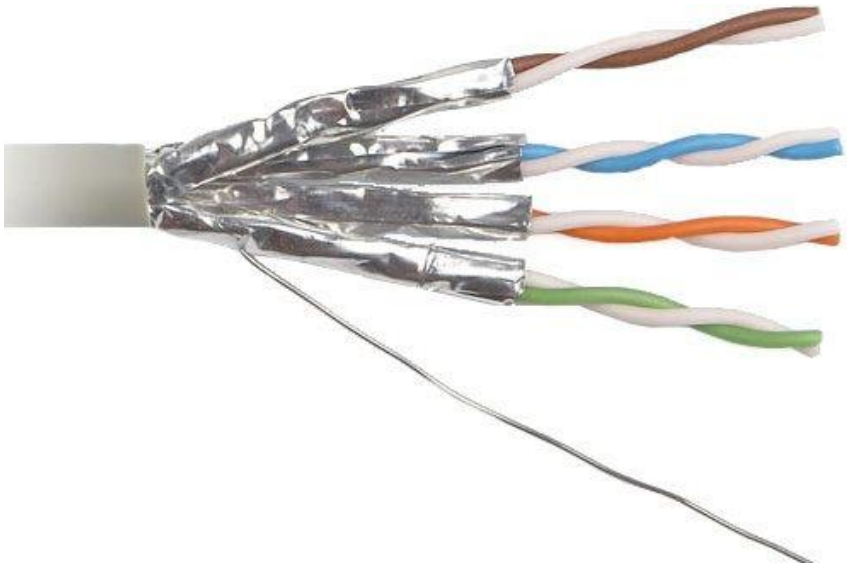
Примеры кабелей (*проводов*), используемых для абонентской проводки.





Кабель типа “витая пара”, используемый для абонентской проводки.





Обозначение кабелей типа “витая пара”.

Обозначение по ISO/IEC 11801	Общий экран	Экран для пар
U/UTP	нет	нет
U/FTP	нет	фольга
F/UTP	фольга	нет
S/UTP	оплётка	нет
SF/UTP	оплётка, фольга	нет
F/FTP	фольга	фольга
S/FTP	оплётка	фольга
SF/FTP	оплётка, фольга	фольга

Буквенный код перед обратной чертой обозначает тип общего экрана для всего кабеля, код после черты обозначает тип индивидуального экранирования для каждой витой пары:

U = unshielded, без экрана

F = foil, фольга

S = braided screening, оплётка из проволоки (только внешний экран)

TP = twisted pair, витая пара

TQ = индивидуальный экран для двух витых пар (на 4 провода)

Примеры экранированных витых пар.

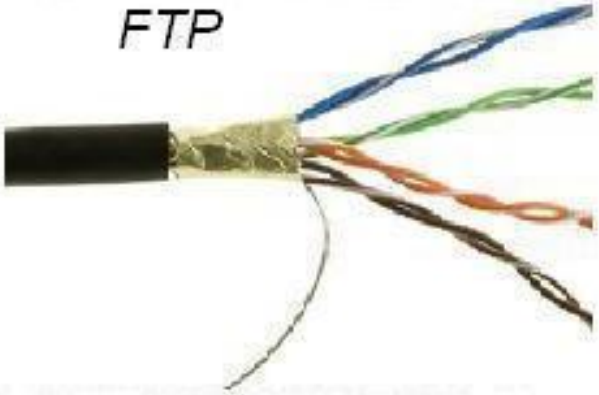
U/FTP

без общего экрана с экранированием каждой пары фольгой

SF/UTP

с двойным общим экраном из оплётки и фольги

FTP

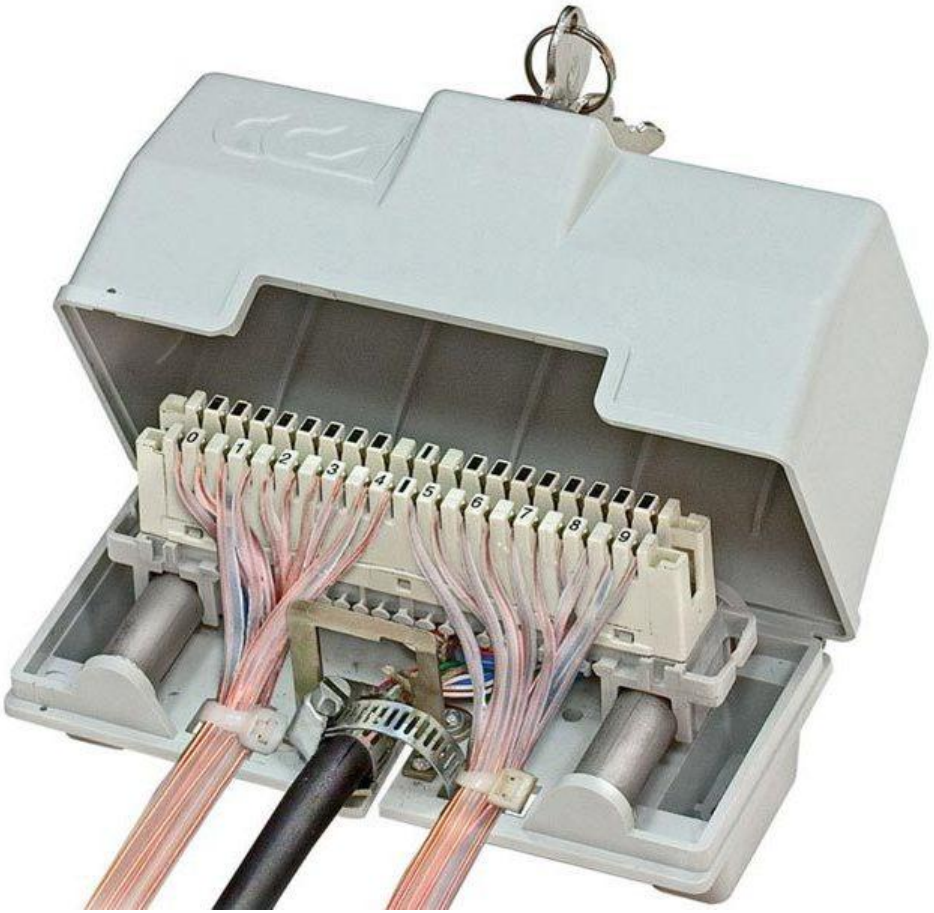


с общим экраном из фольги без экранирования отдельных пар

S/FTP

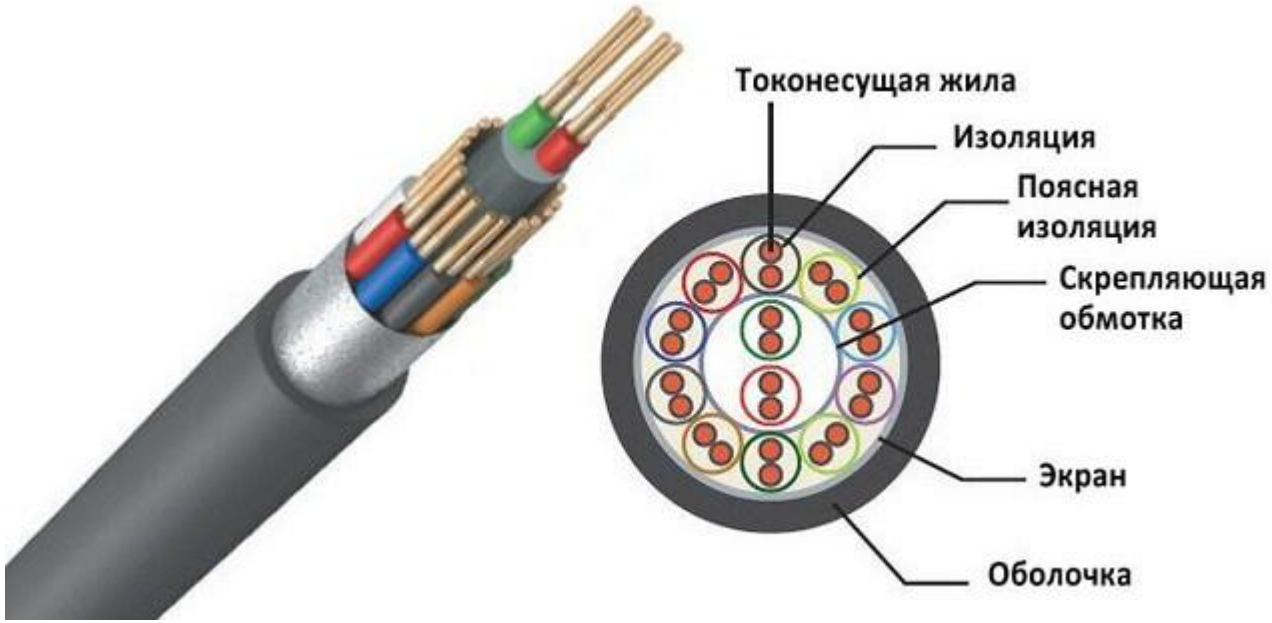
с экранированием каждой пары фольгой и общим плетёным экраном

Примеры абонентских распределительных коробок.

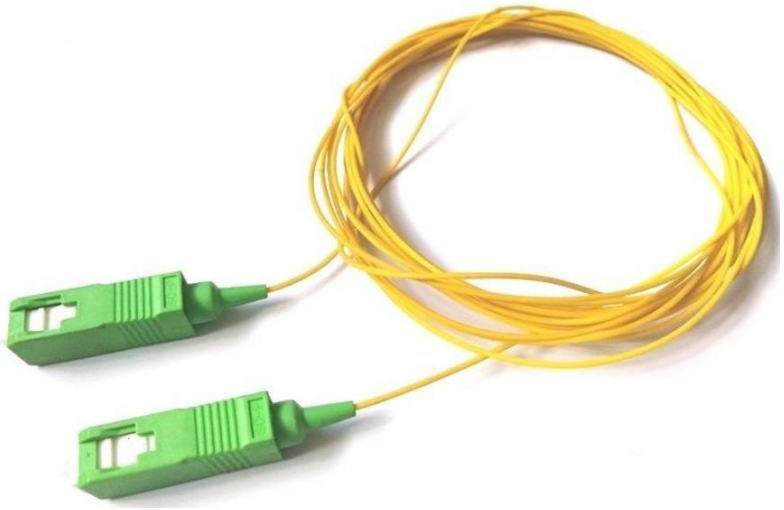


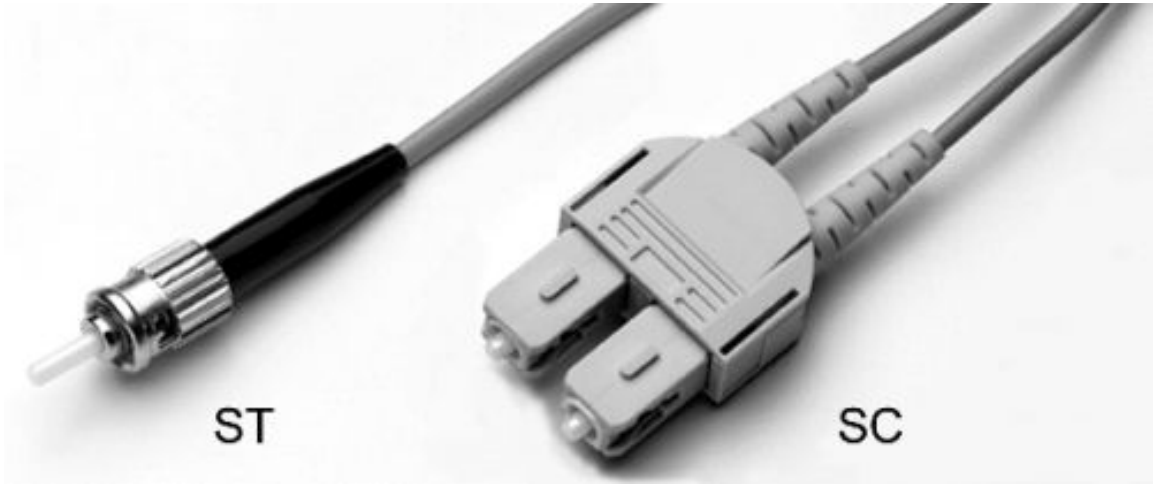
http://ooosd.ru/catalog/2544/50419

Примеры кабелей, используемых на распределительном участке.

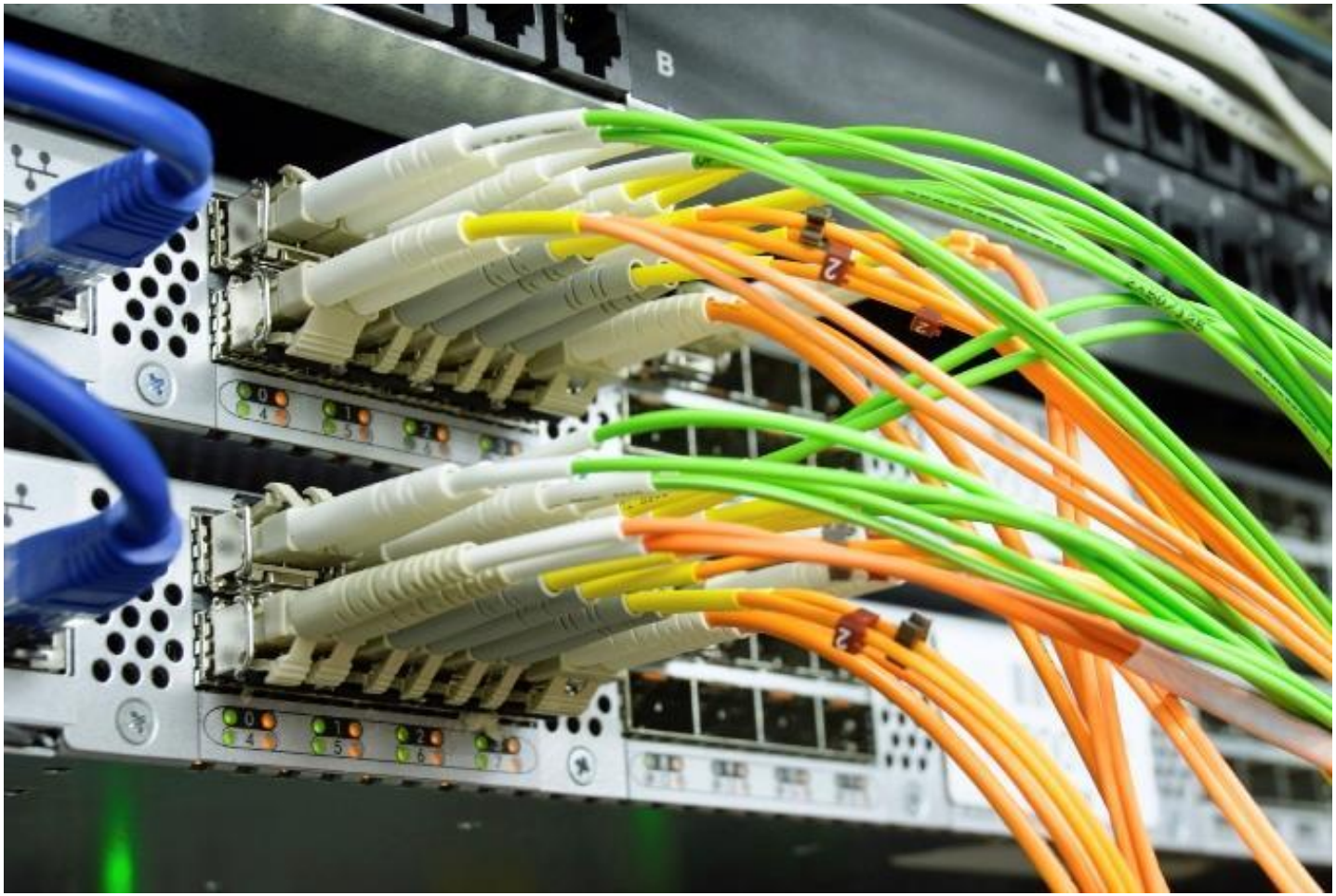


Примеры оптоволоконных кабелей, используемых на распределительном участке и для абонентской проводки.

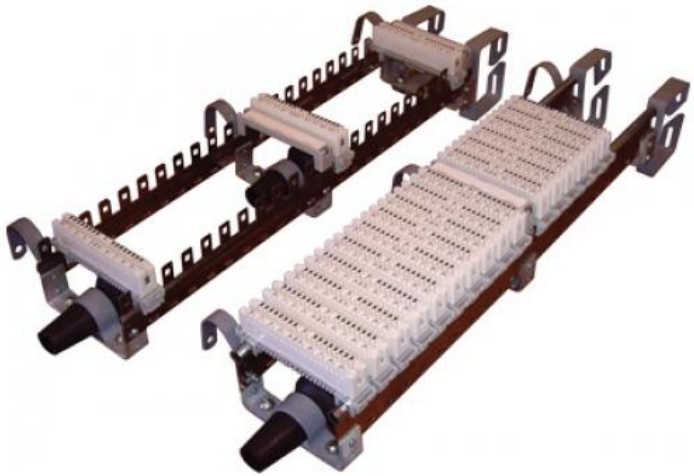


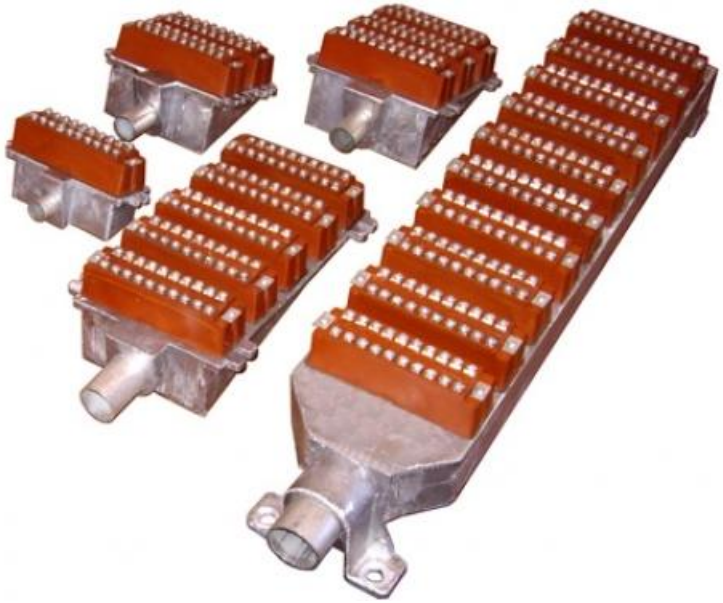


Примеры оптоволоконных кабелей, используемых на распределительном участке и для абонентской проводки.



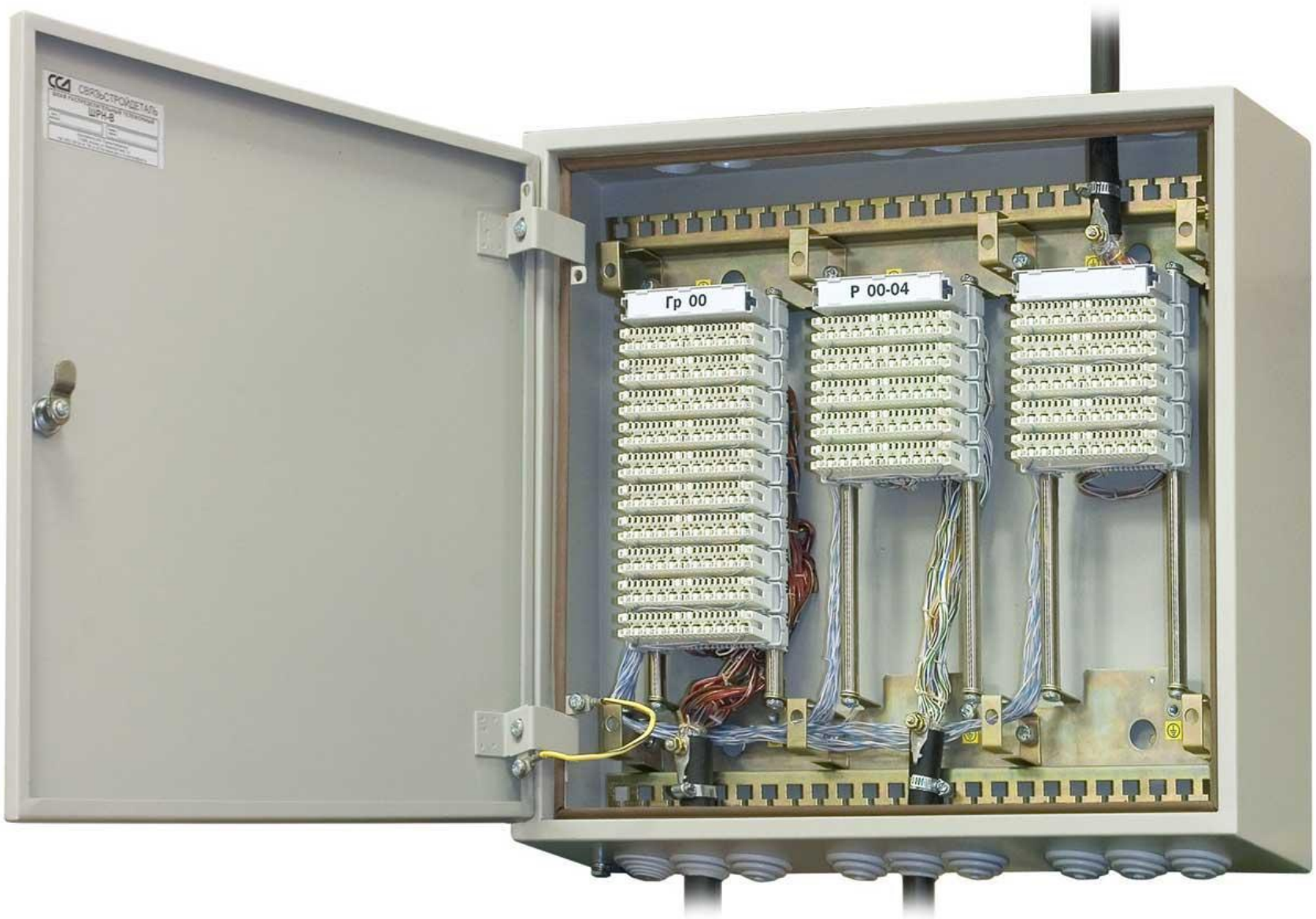
Примеры телефонных распределительных шкафов (*кроссбоксов*).





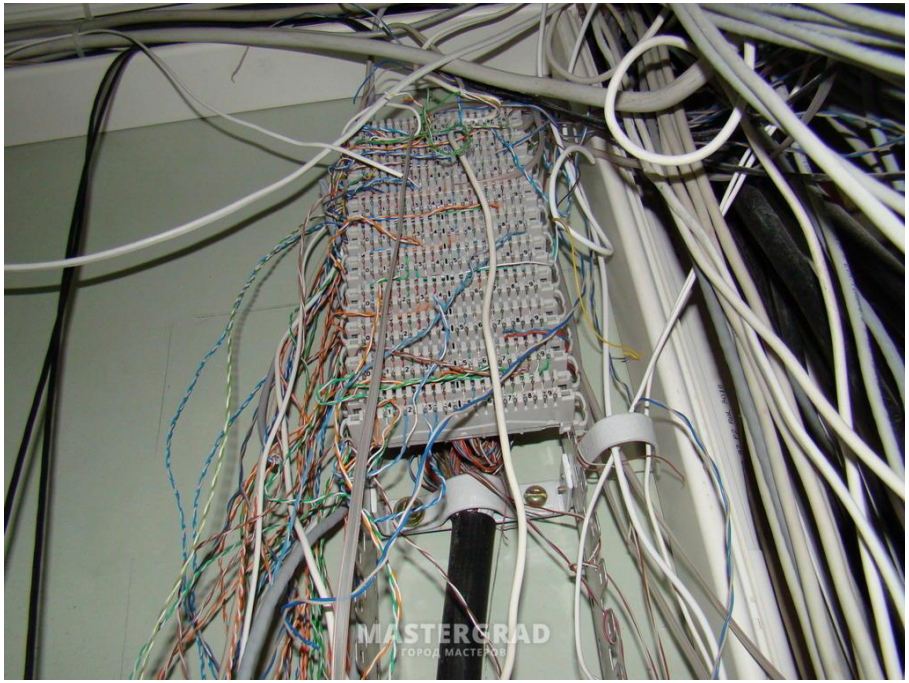
http://ooosd.ru/catalog/2544/50419

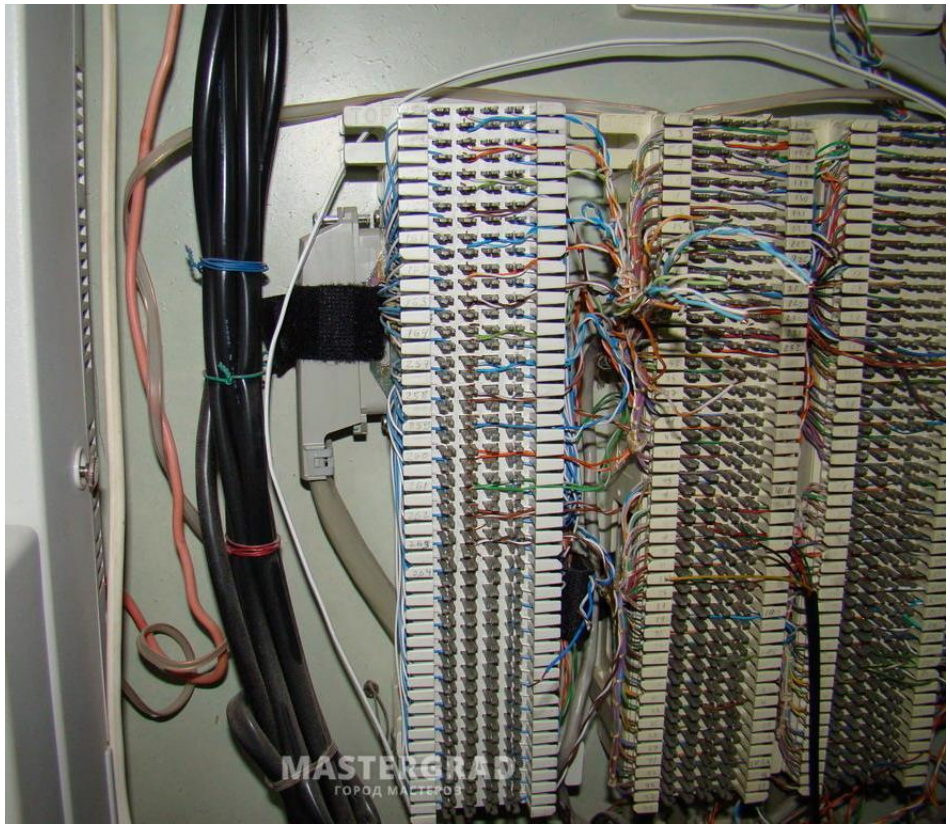
Примеры телефонных распределительных шкафов (*кроссбоксов*).



http://ooosd.ru/catalog/2544/50419

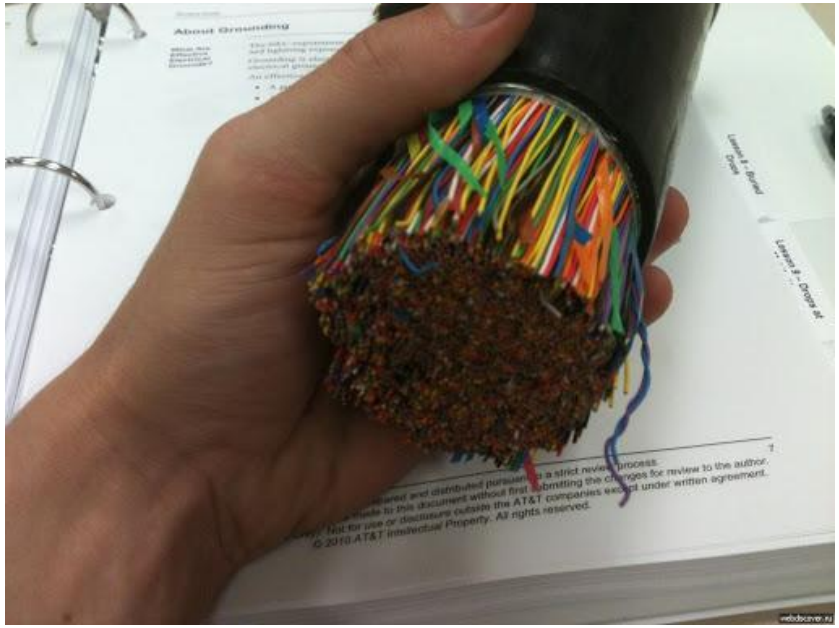
Примеры телефонных распределительных шкафов (*кроссбоксов*).





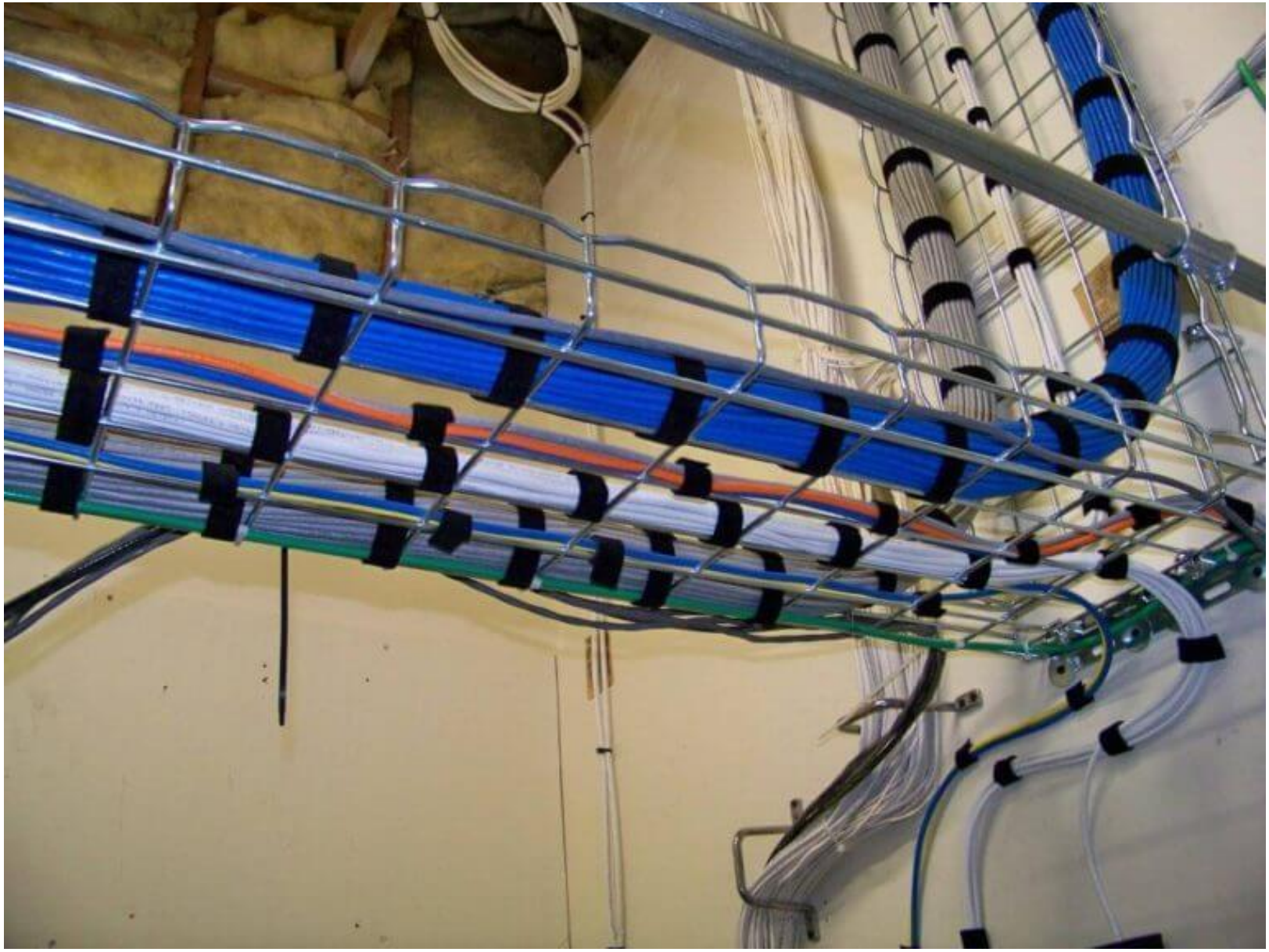
https://mastergrad.com/forums/

Примеры кабелей, используемых на магистральном участке.



Примеры оптоволоконных кабелей, используемых на магистральном участке.

Пример “кабельного хозяйства” на объекте.



Пример типовой городской АТС.

Современные мини-АТС.

В настоящее время большинство компаний и организаций имеют свои собственные АТС (мини-АТС), с помощью которых осуществляется связь как с “внутренними” так и с “внешними” абонентами.
Где-то работают чисто “аналоговые” мини-АТС, где-то – полностью “цифровые” (*включая и абонентские устройства*). Но, как правило, в большинстве случаев используются “гибридные” системы, в которых задействованы как аналоговые, так и цифровые соединения и устройства.
Что касается цифровых систем типа ISDN или VoIP, то в них тоже очень часто используются аналоговые телефонные аппараты, которые “стыкуются” через соответствующий адаптер (*шлюз*).

Использование собственной мини-АТС позволяет снять некоторые “внешние” угрозы – так как телефонная станция и коммутационные устройства теперь находятся на “своей территории”.
Но тут возникает принципиальный вопрос: **кто будет обслуживать мини-АТС**?
Если это “приходящий” сотрудник, то сразу возникает много нюансов.
Если это сотрудник компании, то очень важны его “надёжность” и компетентность, так как именно он может полностью контролировать всё, что касается ведущихся телефонных переговоров (*причём скрытно – со своего рабочего места, используя “дополнительные” возможности АТС*).

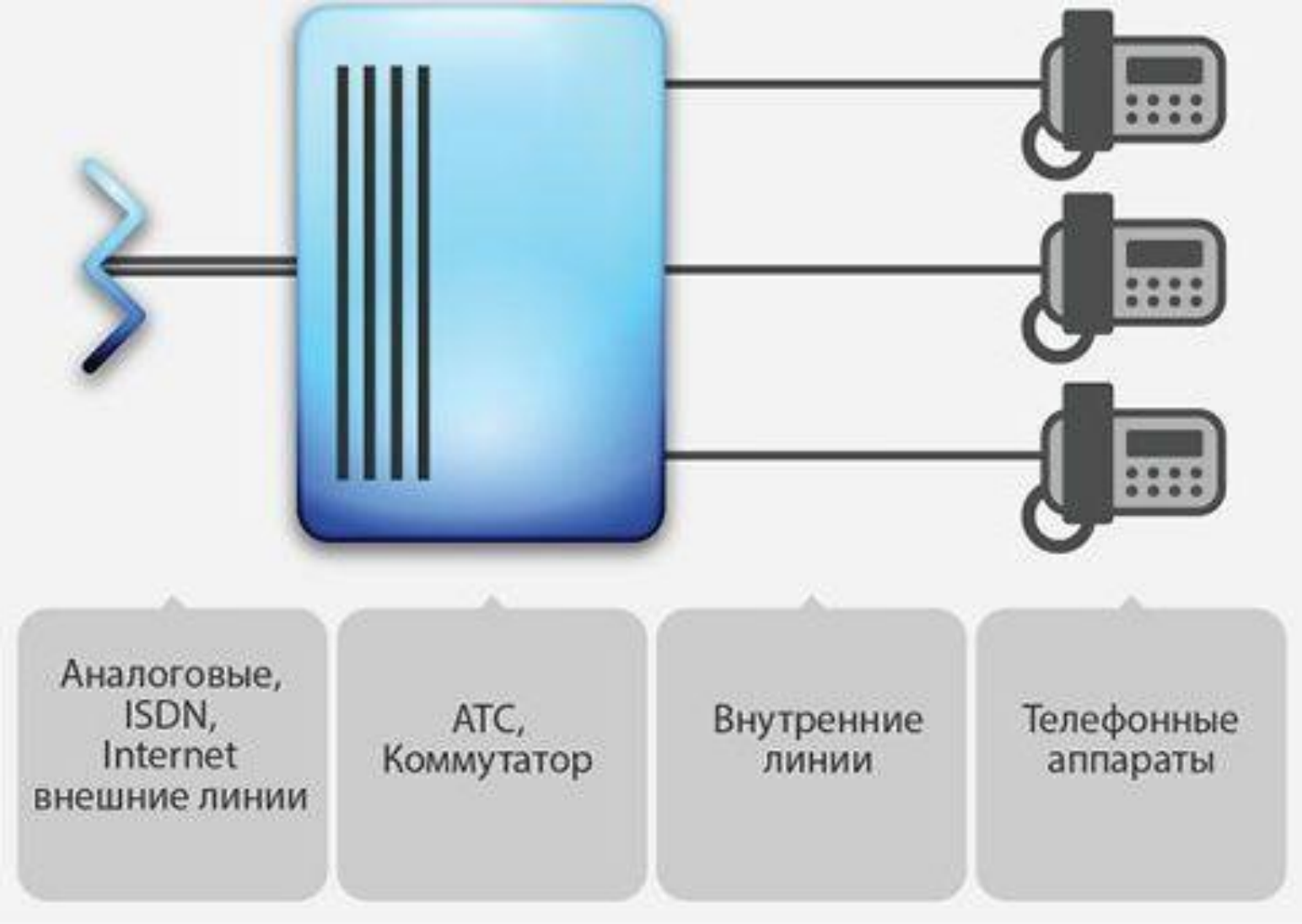
Примеры мини-АТС.

http://ntcpik.com/catalog/telefonnaya-stantsiya/sats-216/

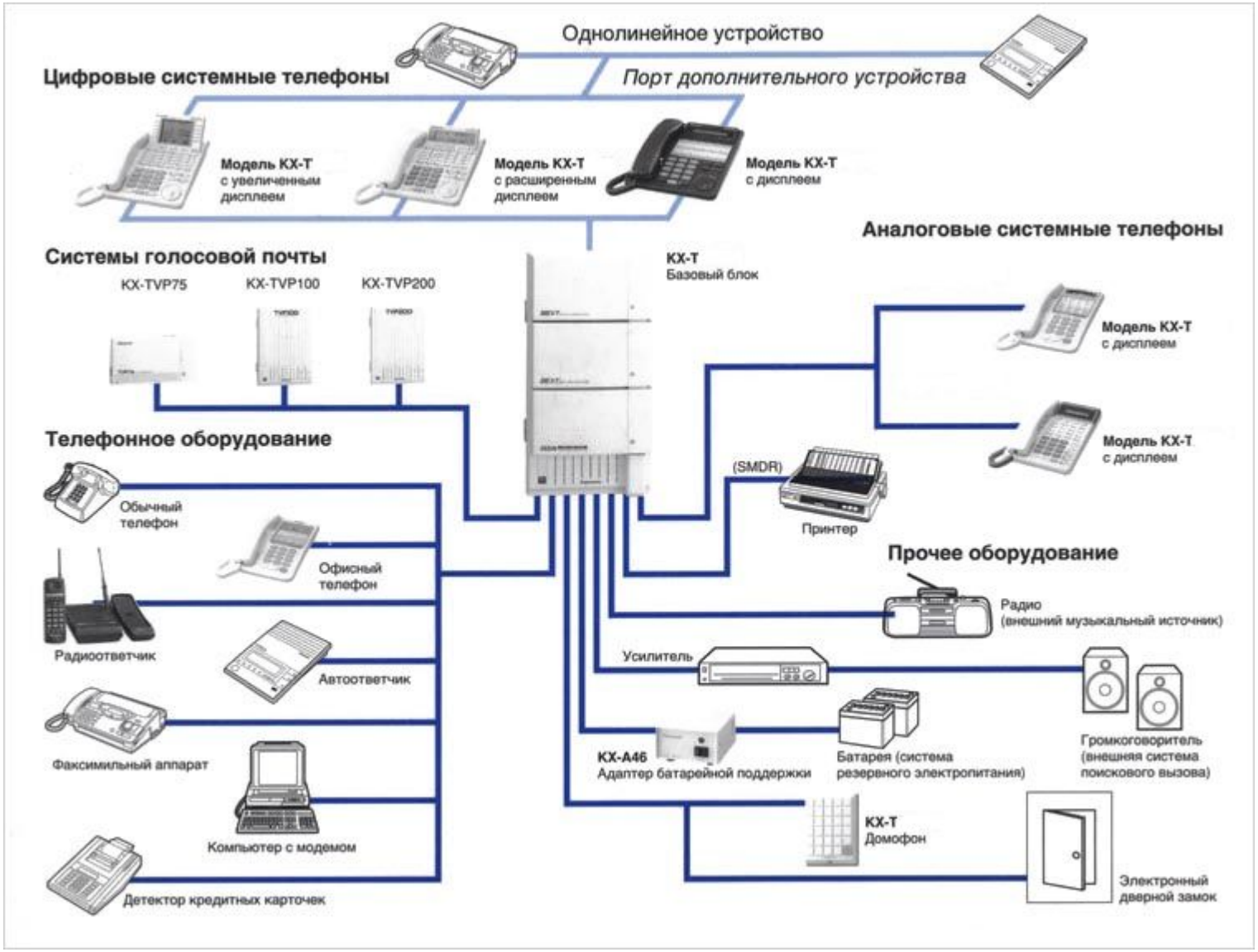
Примеры мини-АТС.

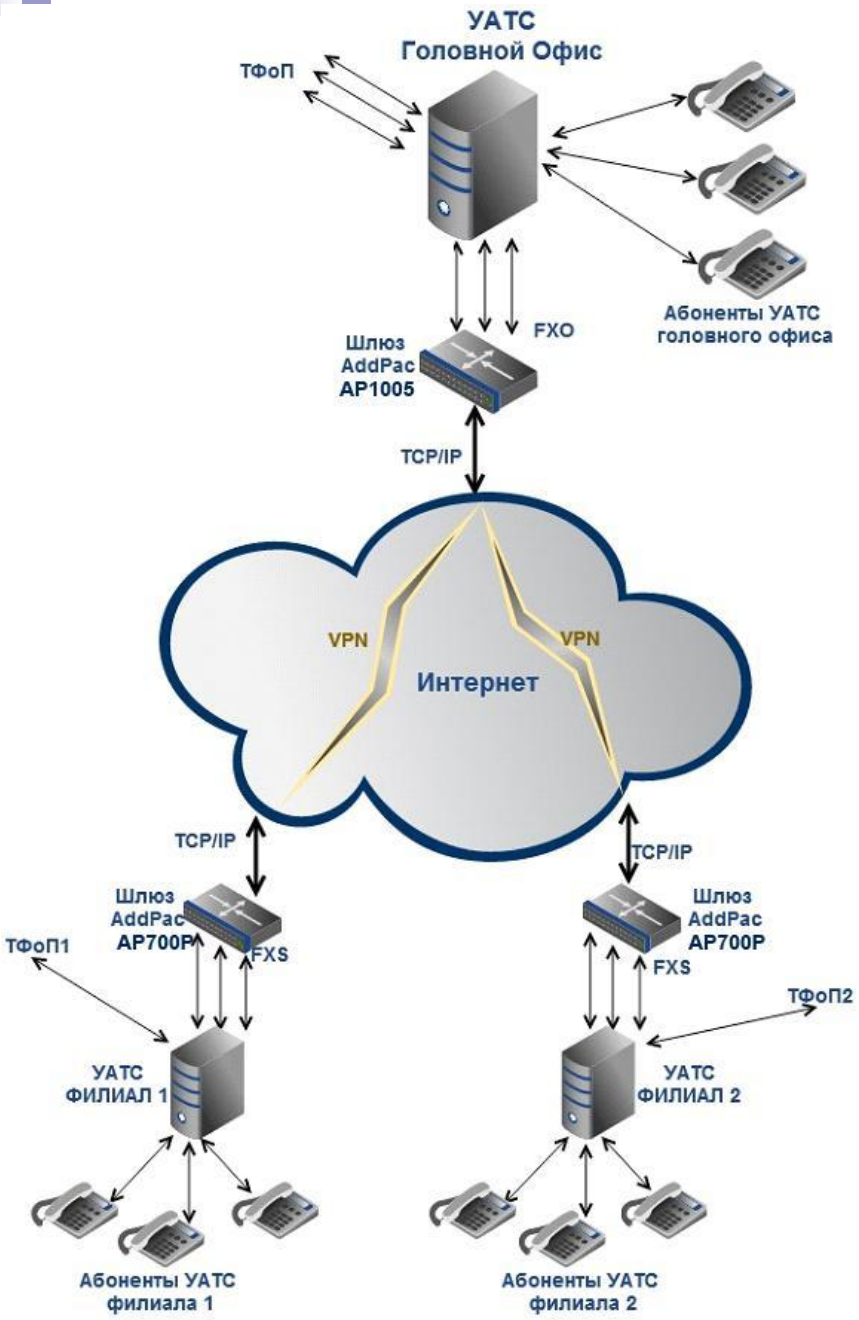
http://www.solarisgroup.ru/panasonic_kx_tde100/

Принципиальная схема типовой мини-АТС.



Типовая схема офисной мини-АТС, к которой подключены как “аналоговые”, так и “цифровые” абонентские устройства.

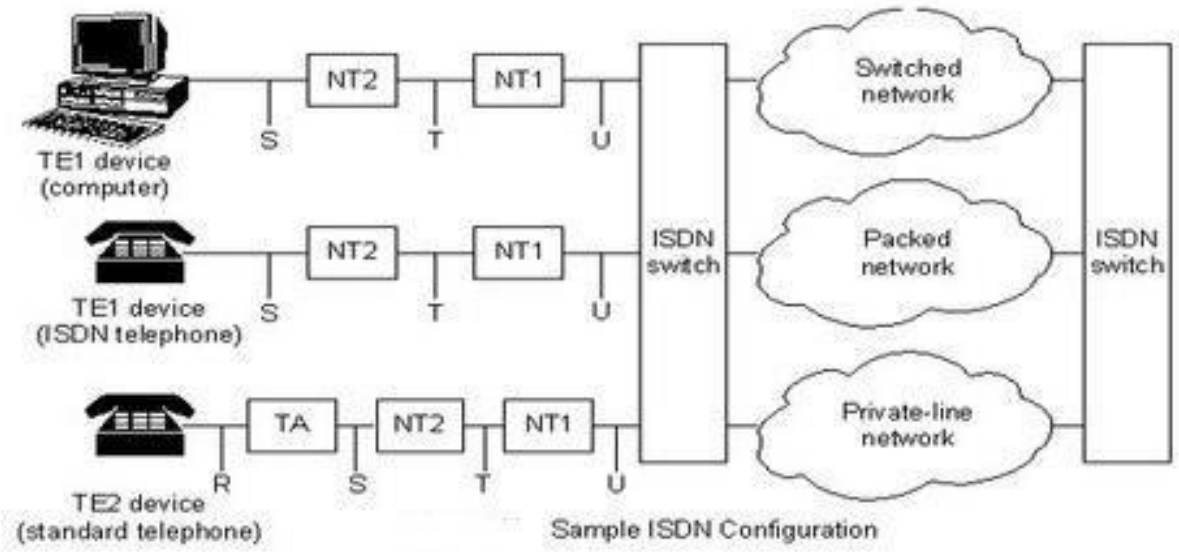


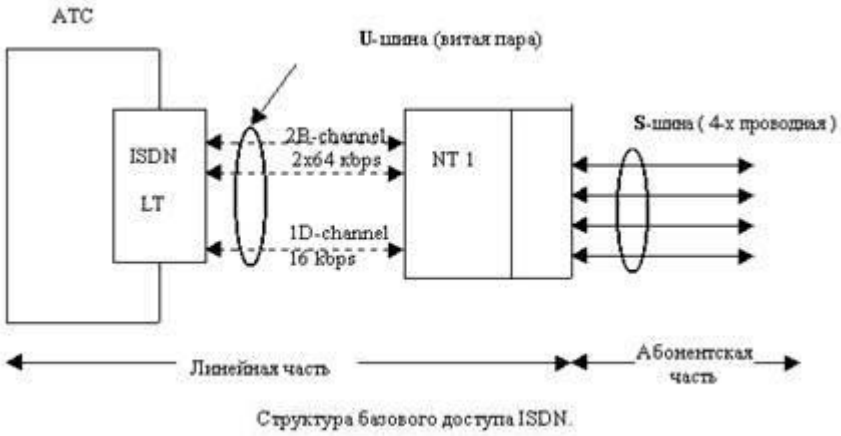


Типовая схема построения корпоративной сети связи на базе мини-АТС.

При наличии в компании (*организации*) нескольких территориально-разнесённых подразделений (*филиалов*) они могут быть соединены между собой (*например, с помощью VPN*) и будут “замыкаться” на одну АТС. При этом телефонные разговоры между абонентами компании будут “внутренними” (*бесплатными*), даже если физически они находятся в различных городах (*странах*).

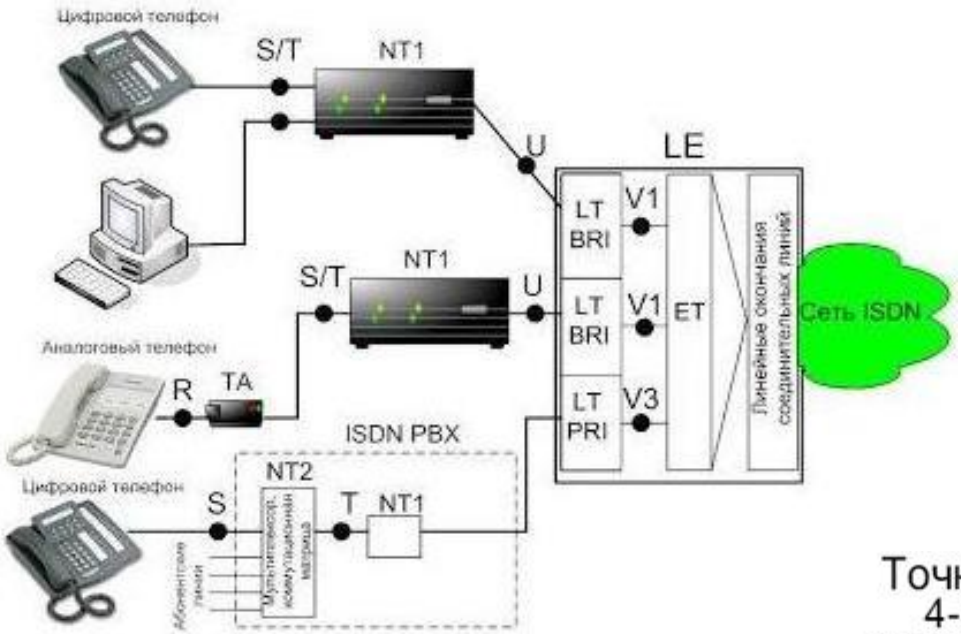
Принцип построения и особенности ISDN сети.

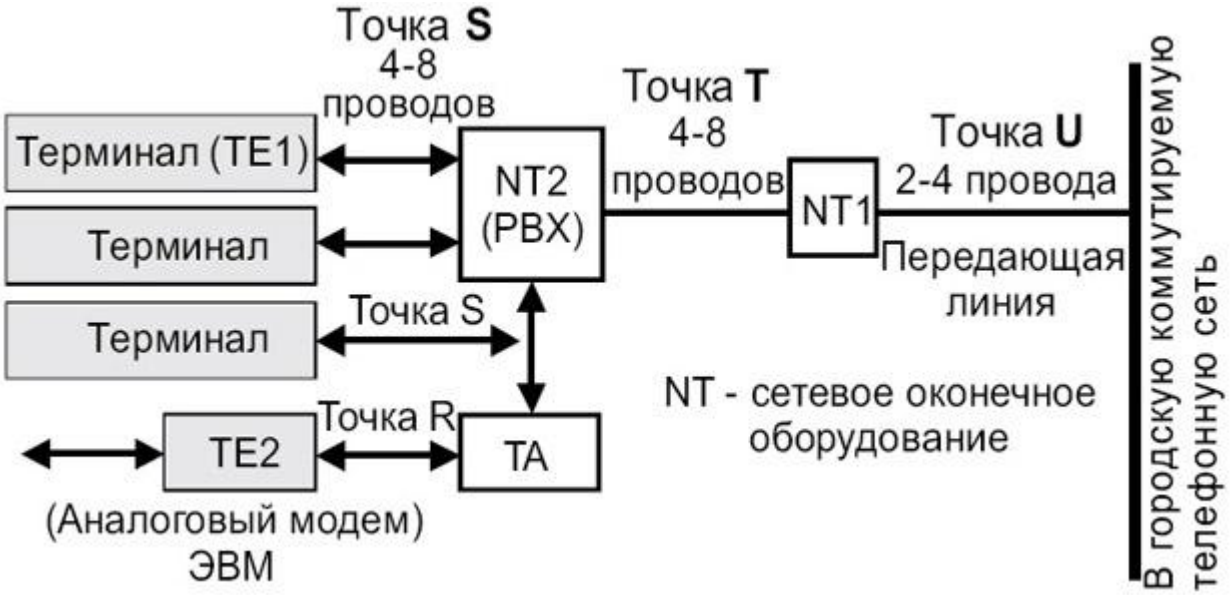




Структура базового доступа ISDN.

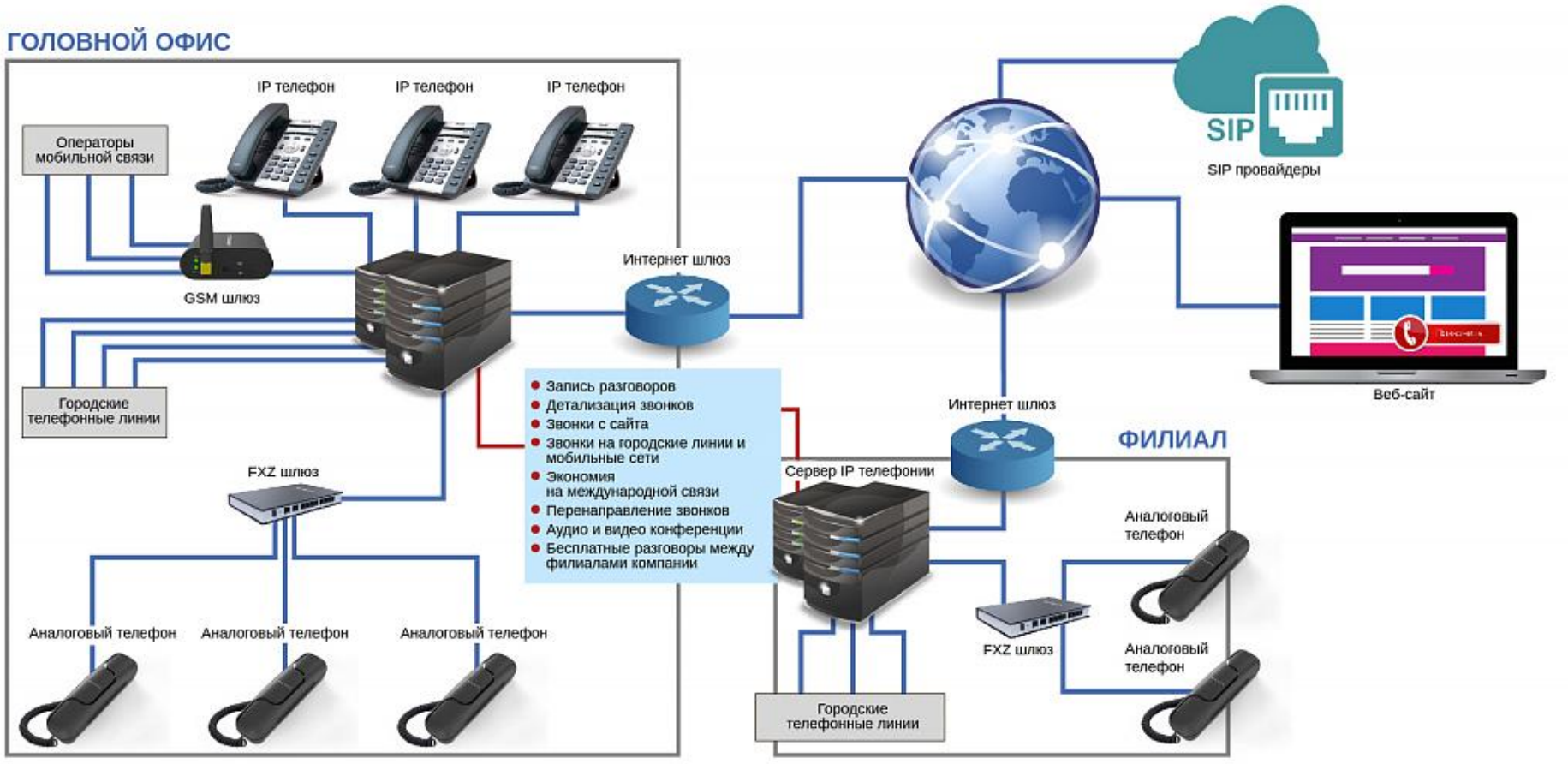
Варианты подключения устройств и опорные точки ISDN.



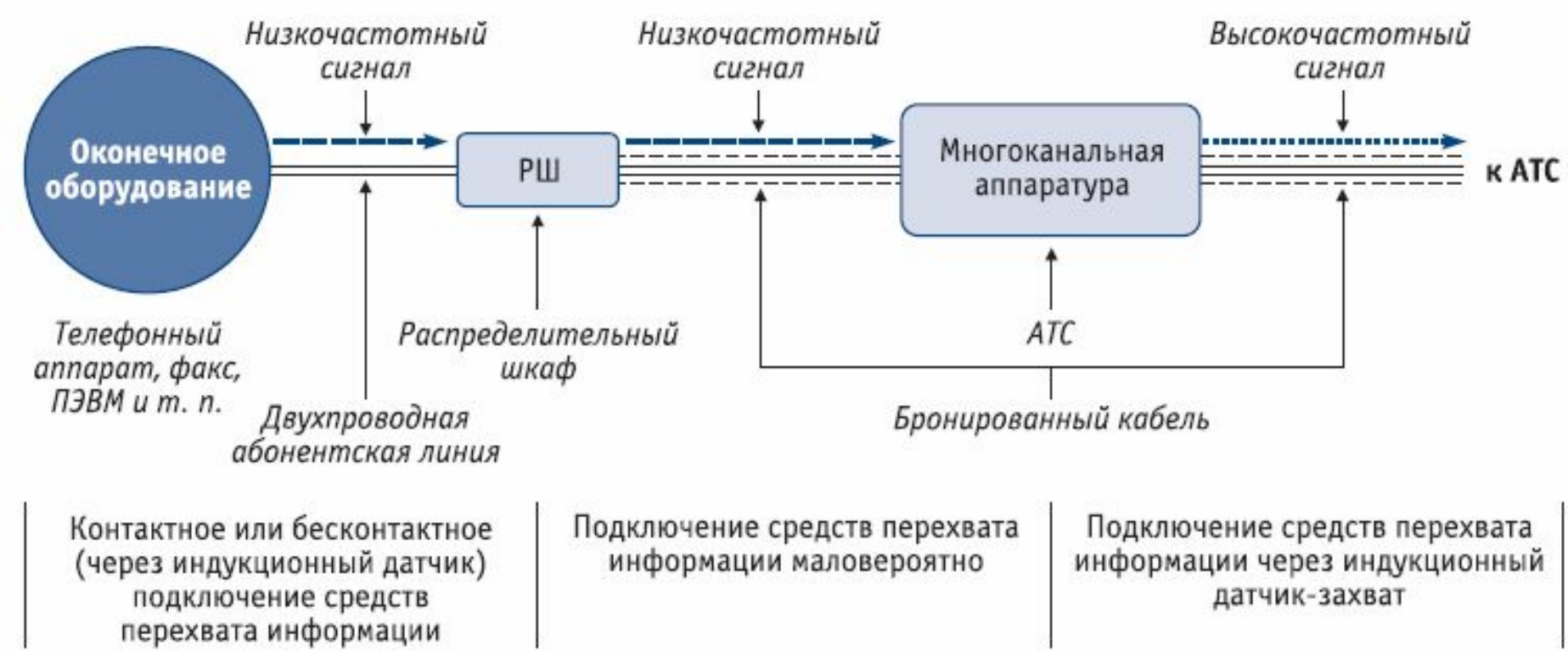


Принцип построения VoIP систем.

Пример VoIP системы.



Возможные места подключения к телефонной линии.



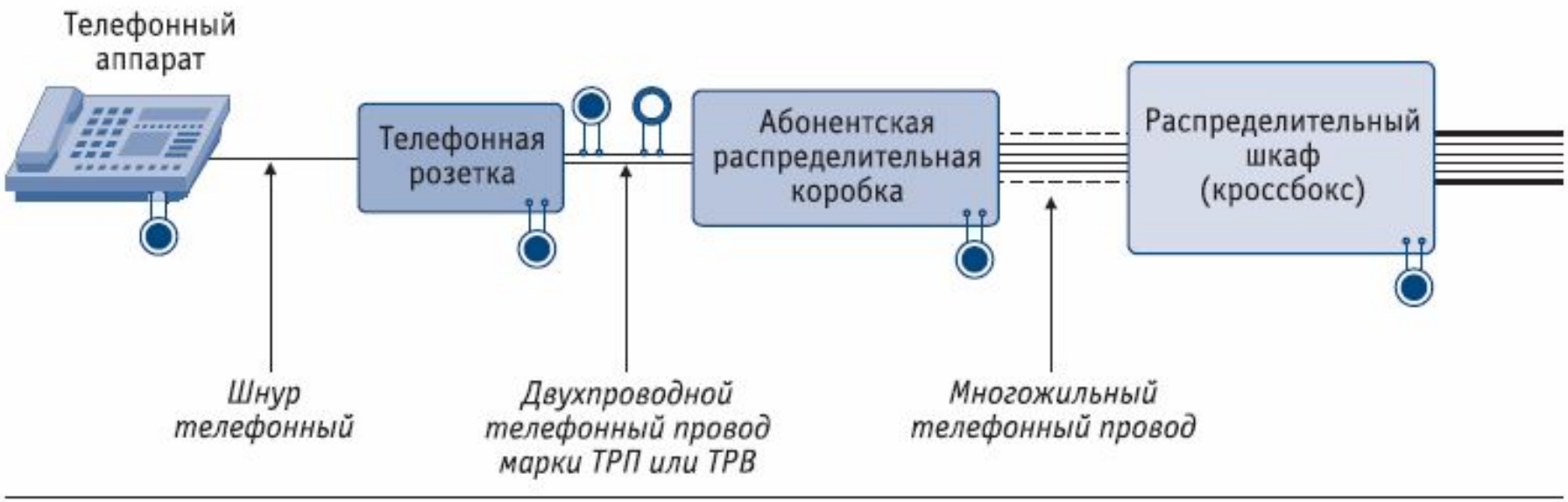
Структура обычной абонентской линии городской телефонной сети включает в себя:

- магистральный участок (от кросса АТС до распределительного шкафа, установленного в жилом или административном здании);
- распределительный участок (от распределительного шкафа до распределительной коробки);
- абонентскую проводку (от распределительной коробки до розетки телефонного аппарата).

Использование тех или иных средств перехвата информации, передаваемой по телефонным линиям связи, будет определяться возможностью доступа к линии связи.

Хорев А.А. Техническая защита информации: учеб. пособие для студентов вузов. В 3 т., Т. 1. Технические каналы утечки информации. − М.: ООО «НПЦ Аналитика», 2008.

Возможные места подключения средств перехвата информации на участке абонентской линии от распределительного шкафа до ТА.



– места возможного контактного подключения средств перехвата информации;

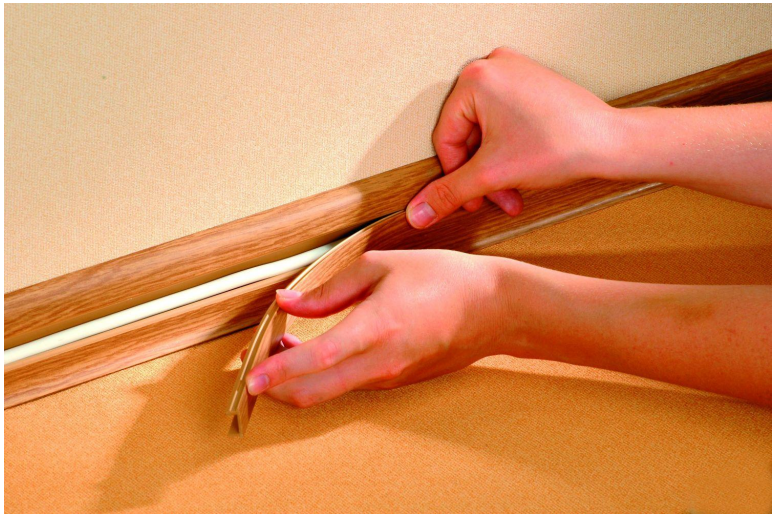
– места возможного бесконтактного (через индукционный датчик) подключения средств перехвата информации

Распределительный участок телефонной линии и абонентская проводка являются наиболее вероятными участками подключения средств перехвата информации. Средства съёма информации могут быть установлены: в телефонном аппарате, в телефонной розетке, в абонентских распределительных коробках, в распределительных шкафах, а также непосредственно на абонентской проводке.

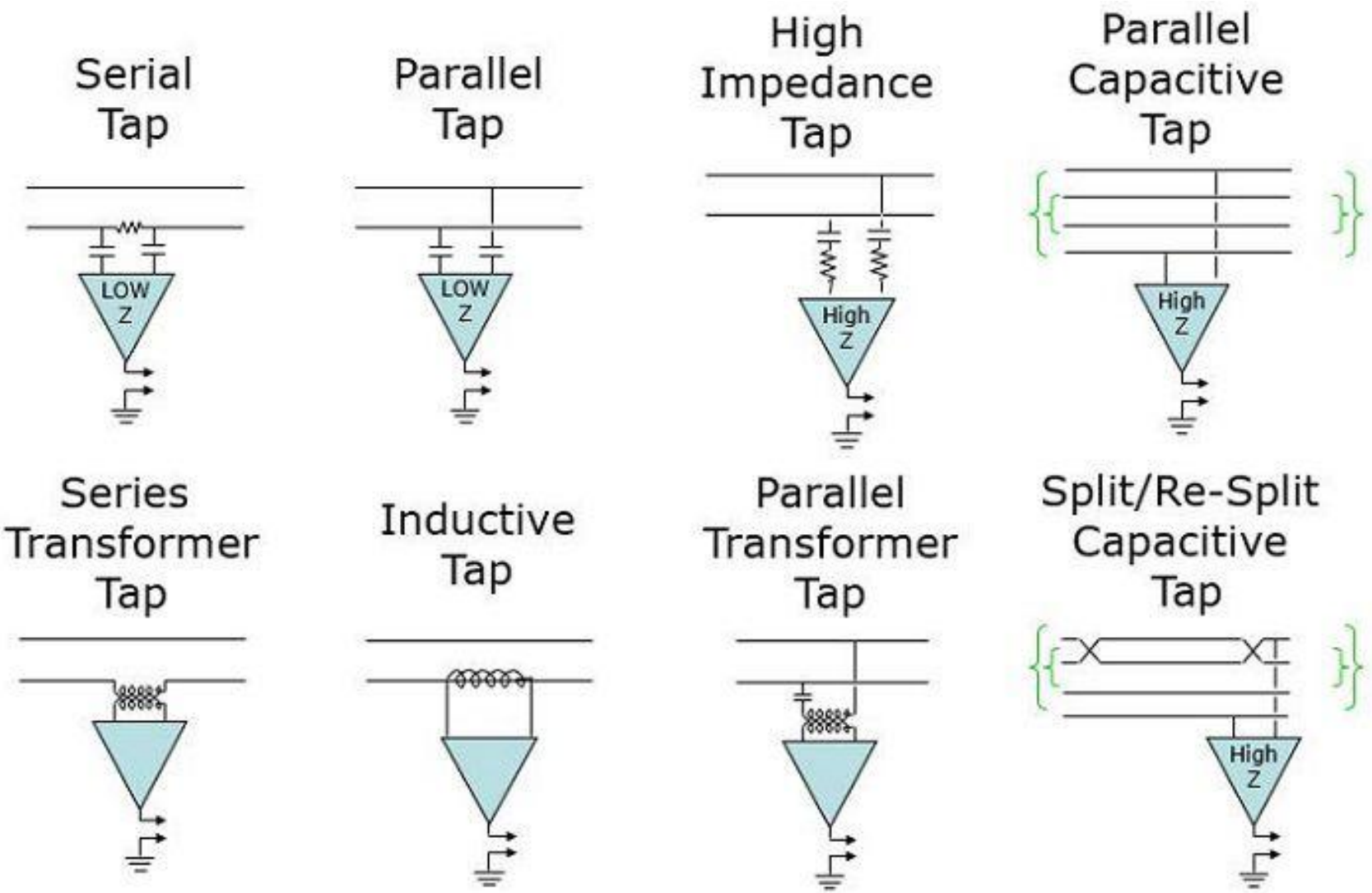
Хорев А.А. Техническая защита информации: учеб. пособие для студентов вузов. В 3 т., Т. 1. Технические каналы утечки информации. − М.: ООО «НПЦ Аналитика», 2008.

Некоторые места возможной установки средств съёма информации на абонентском участке телефонной линии.

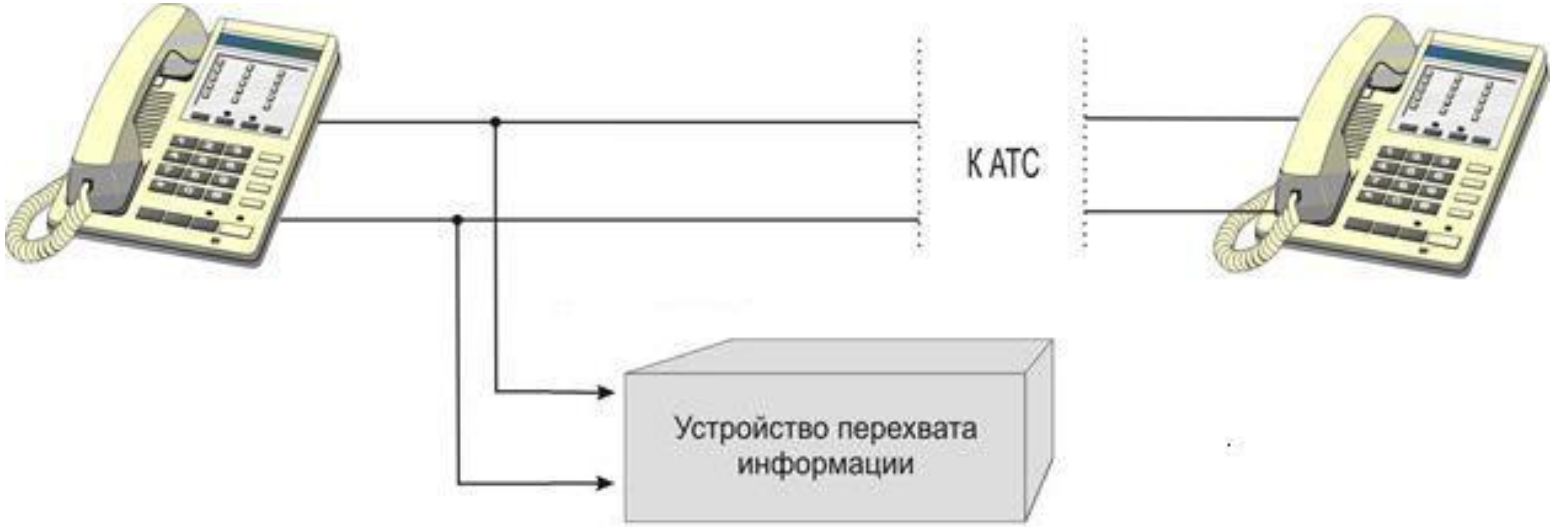
Современные кабель-каналы могут быть использованы для установки различных средств съёма информации, передаваемой по телефонной линии.
В зависимости от конкретной ситуации, подключение к линии может быть произведено в различных точках пробега “нужного” кабеля.

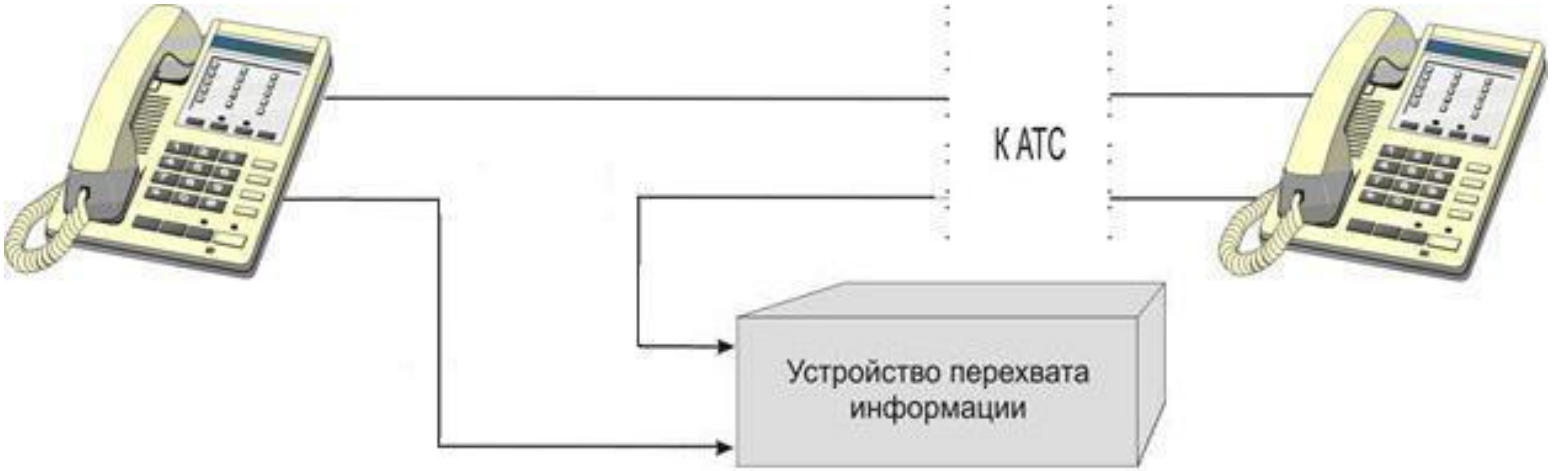


Различные схемы возможного подключения к телефонной линии.



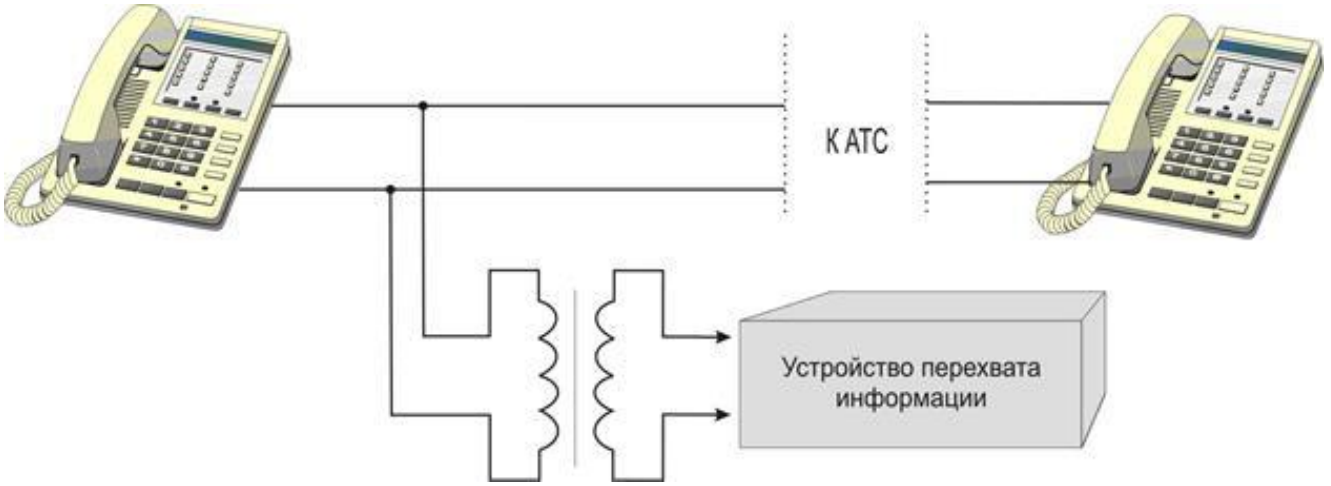
Принцип контактного подключения к телефонной линии.

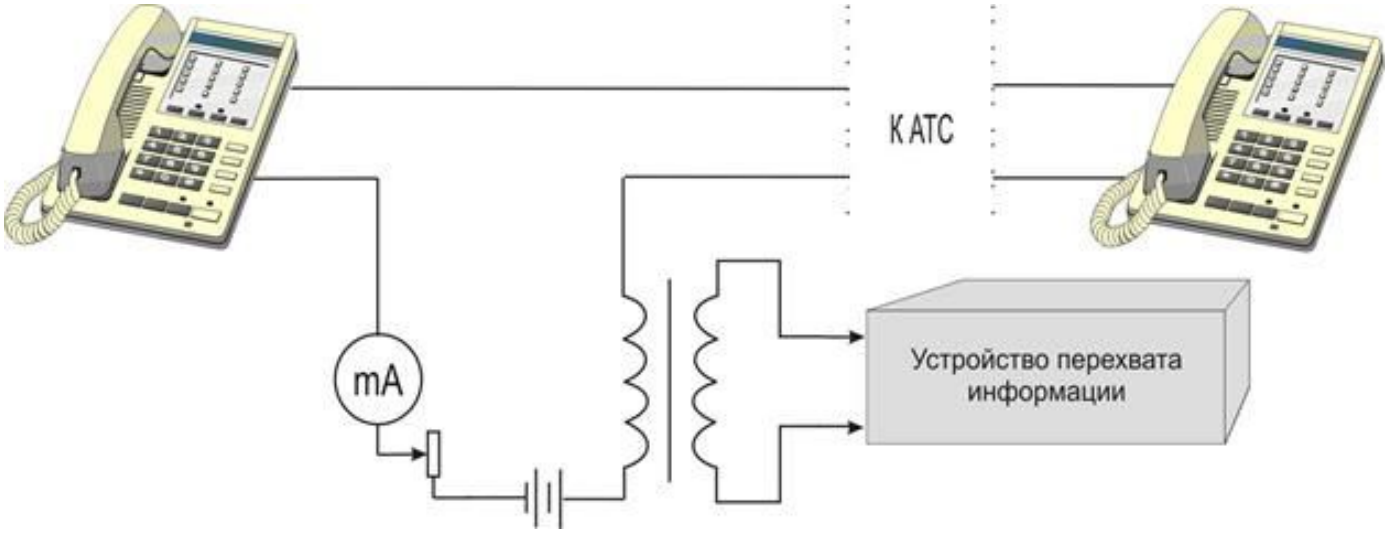




https://studfile.net/preview/1714431/page:10/

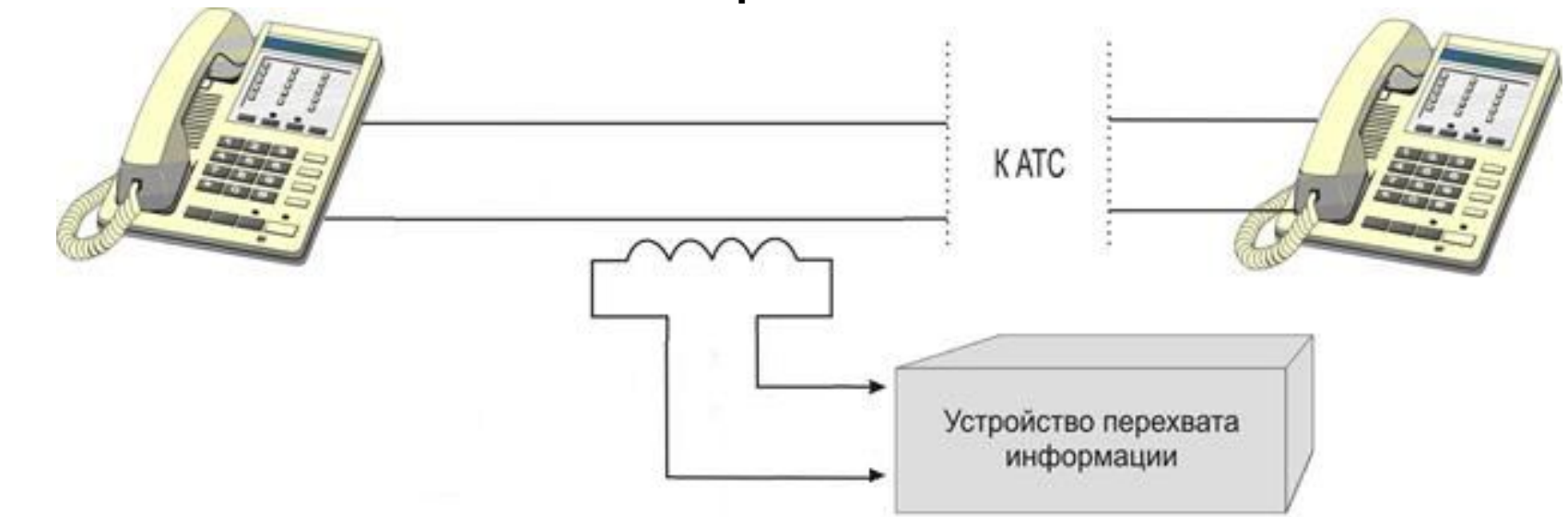
Принцип контактного подключения к телефонной линии через согласующий трансформатор и с компенсацией падения напряжения.

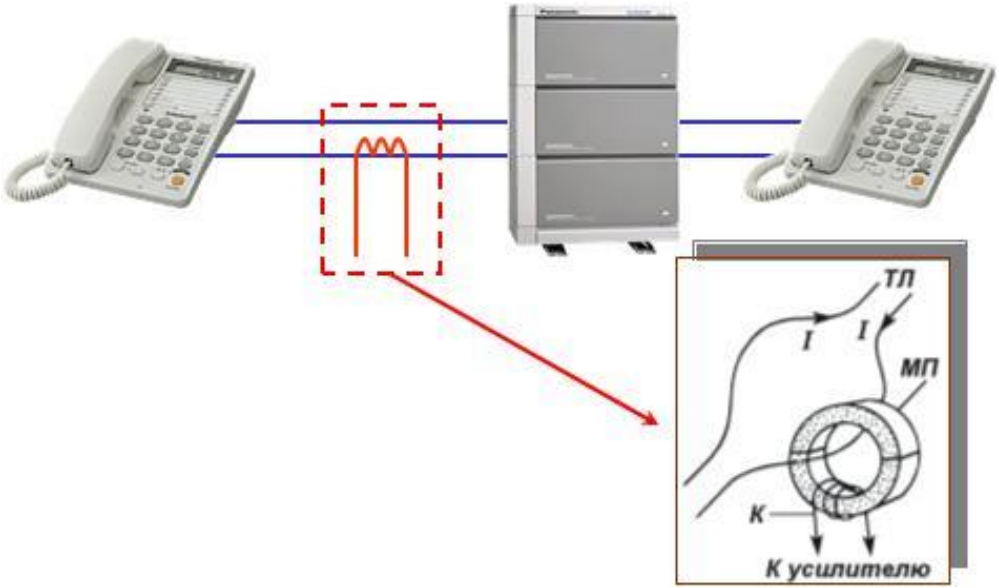




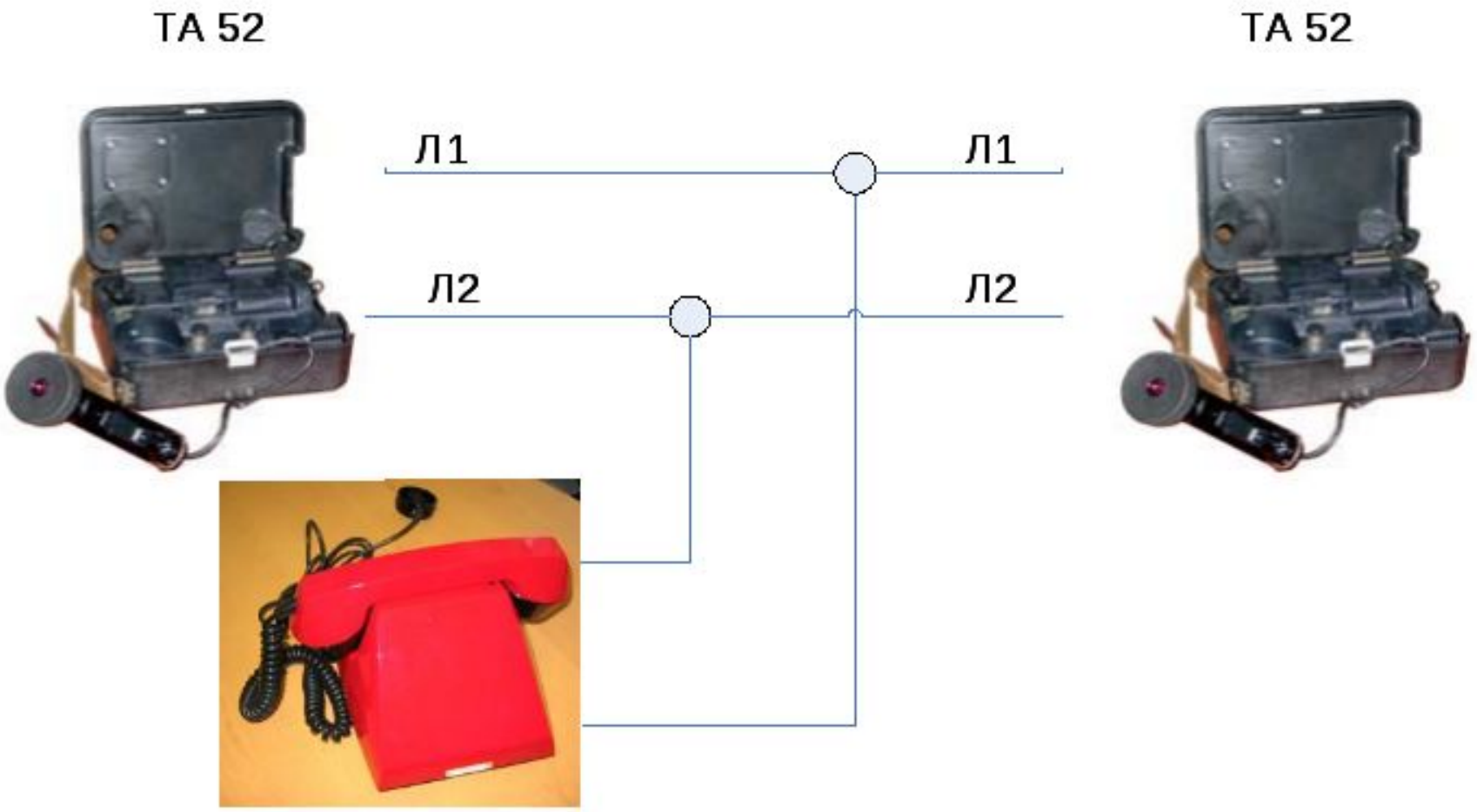
https://studfile.net/preview/1714431/page:10/

Принцип бесконтактного (*индукционного*) подключения к телефонной линии.





Прослушивание телефонных переговоров с помощью “параллельного” телефонного аппарата или “трубки монтёра”.



https://studfile.net/preview/2384014/page:2/

Прослушивание телефонных переговоров с помощью “параллельного” телефонного аппарата.

Примеры телефонных “монтёрских” трубок.

Подключение к линии с помощью телефонного адаптера.

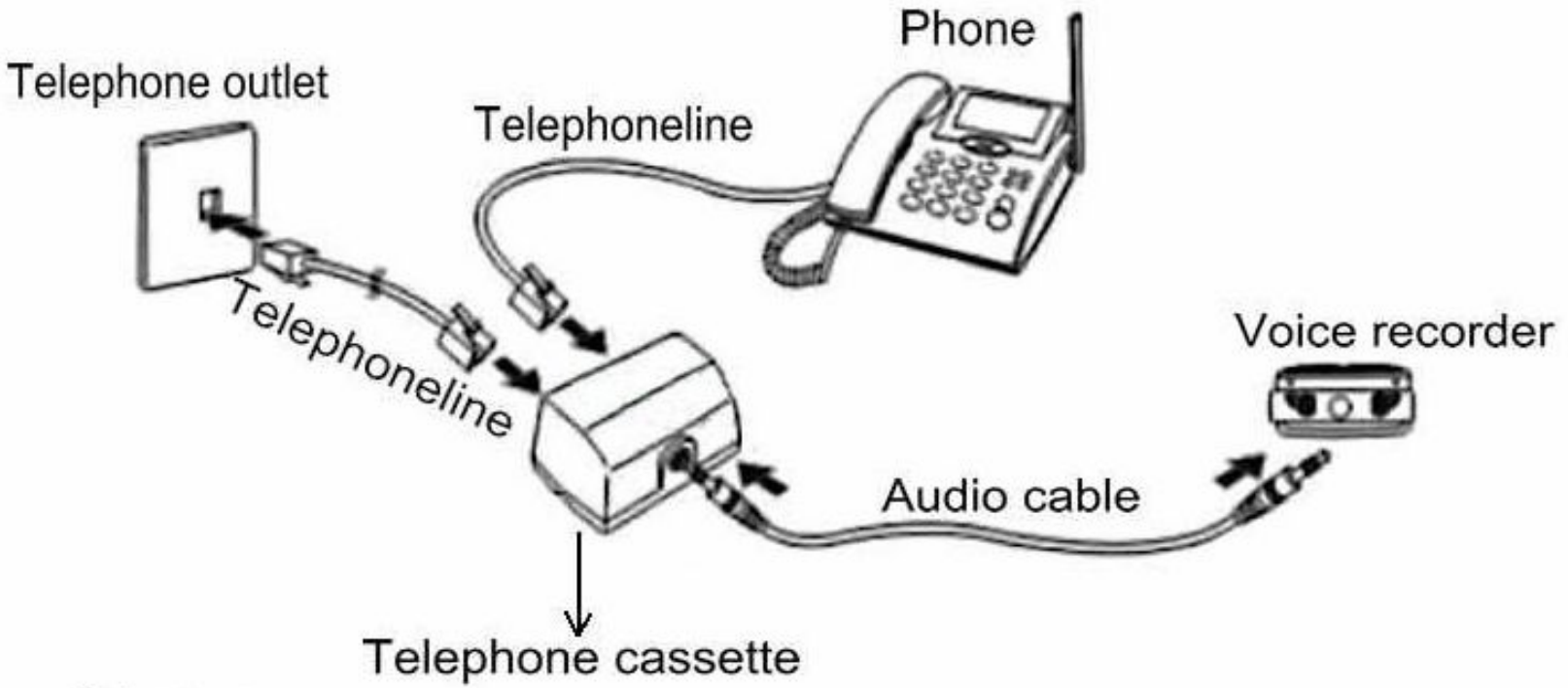
Телефонные адаптеры получили широкое распространение в конце девяностых – начале двухтысячных.
В то время они активно использовались для подключения диктофонов к телефонной линии – в том числе, для записи “своих” телефонных разговоров на “своём” стационарном телефоне.
В настоящее время, в связи с массовым появлением систем записи телефонных переговоров (*см. далее*), адаптеры стали не так актуальны, но они по прежнему имеются в достаточно большом “ассортименте” – как новые модели, так и “из старых запасов”.

По способу подключения к линии можно выделить два типа адаптеров: с гальваническим подключением (*параллельно или в разрыв*) и с индукционным подключением.

Как правило, телефонный адаптер изготавливается в виде отдельного устройства (*модуля*), но существуют модели диктофонов (*магнитофонов*) с уже встроенным телефонным адаптером.
Необходимо отметить, что существуют адаптеры для подключения к “цифровым” линиям – *например, ISDN и VoIP*.

Принцип работы “классического” телефонного адаптера.

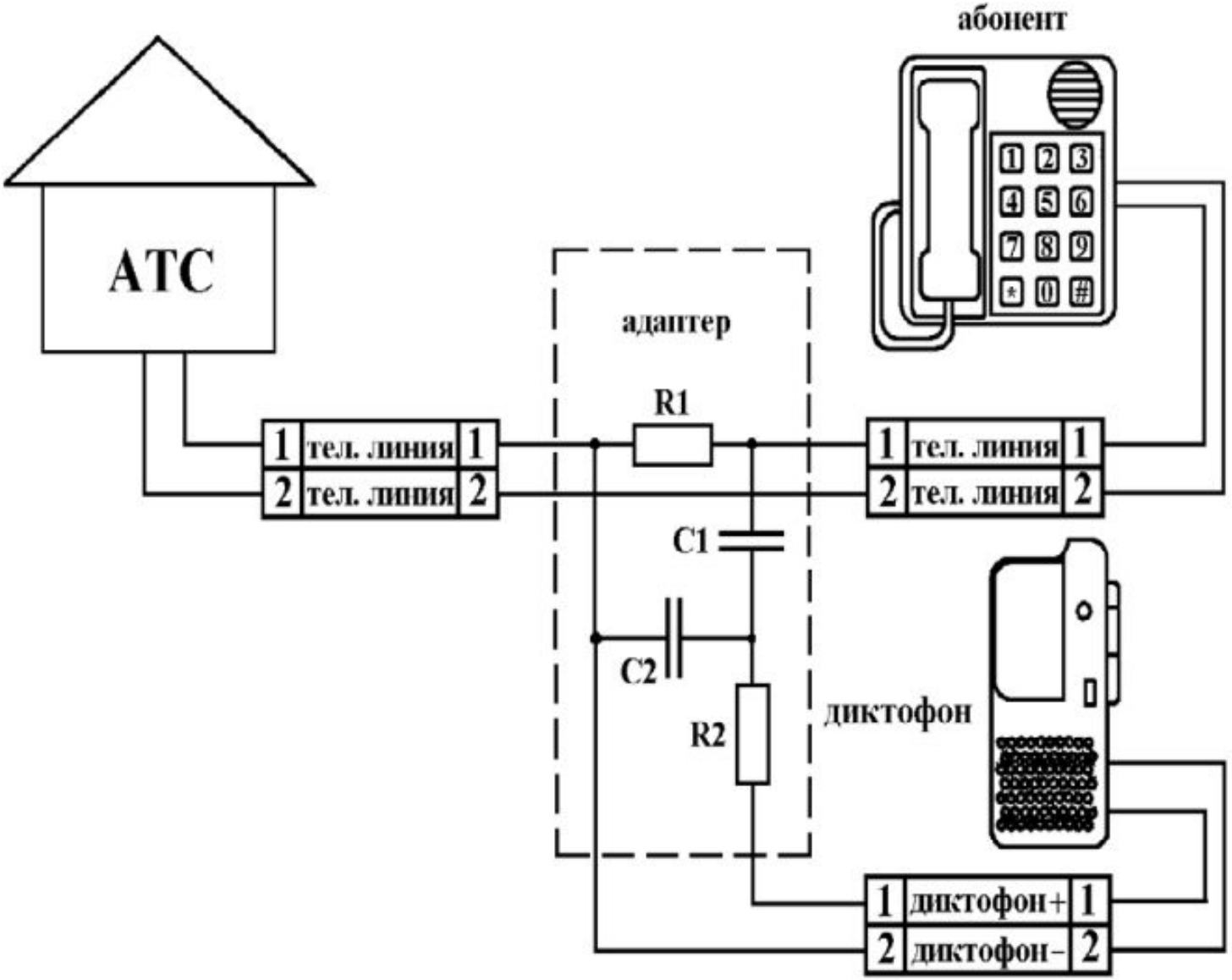
How to connect telephone cassette?



Steps:

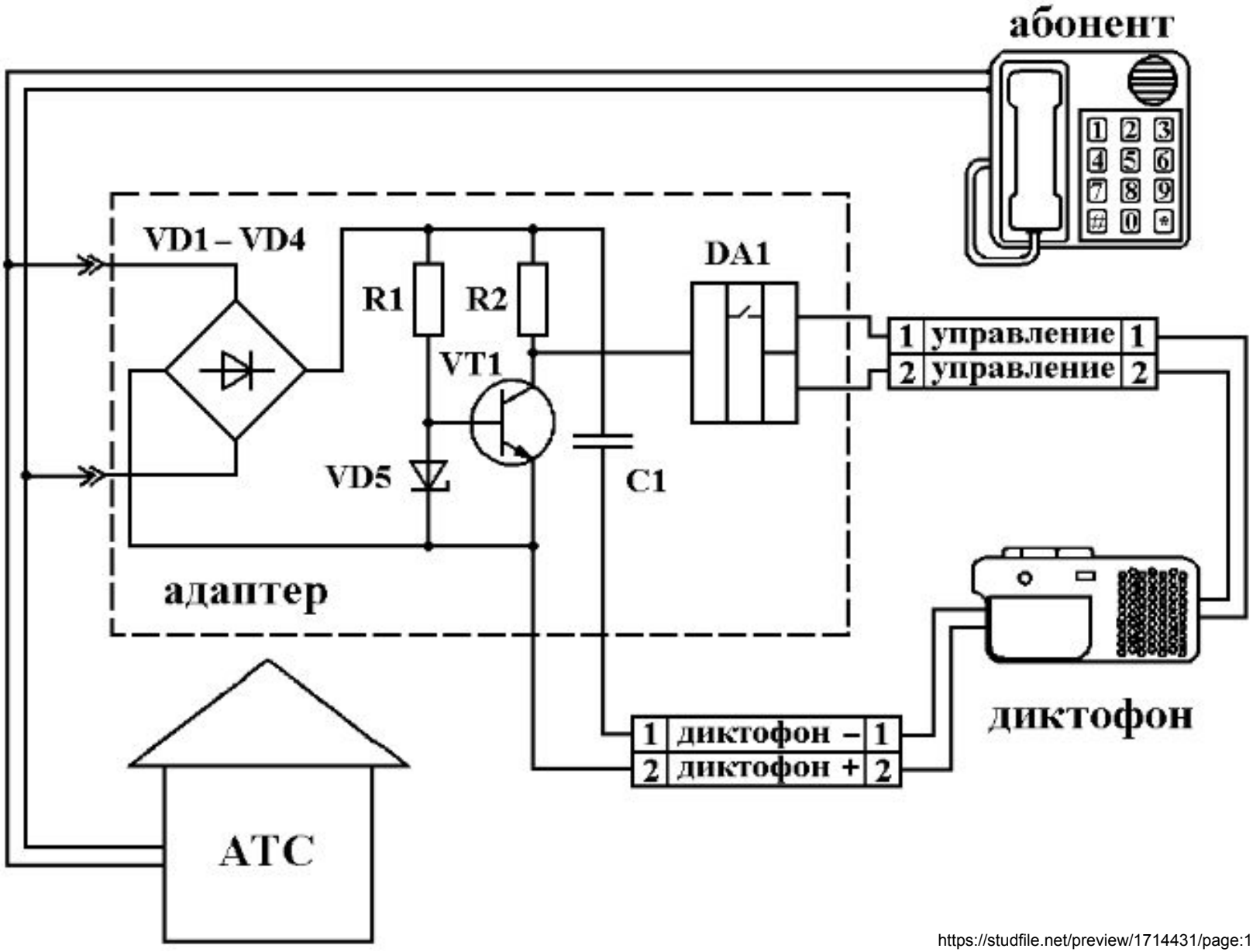
1. Connect the telephone cassette and your phone via telephoneline.
2. Connect the telephone cassette and the telephone via telephoneline.
3. Connect the tephone cassette and your voice recorder via audio cable.
4. Press "Record" button on your voice recorder to sync recording.

Схема телефонного адаптера с последовательным подключением.



https://studfile.net/preview/1714431/page:10/

Схема телефонного адаптера с параллельным подключением.

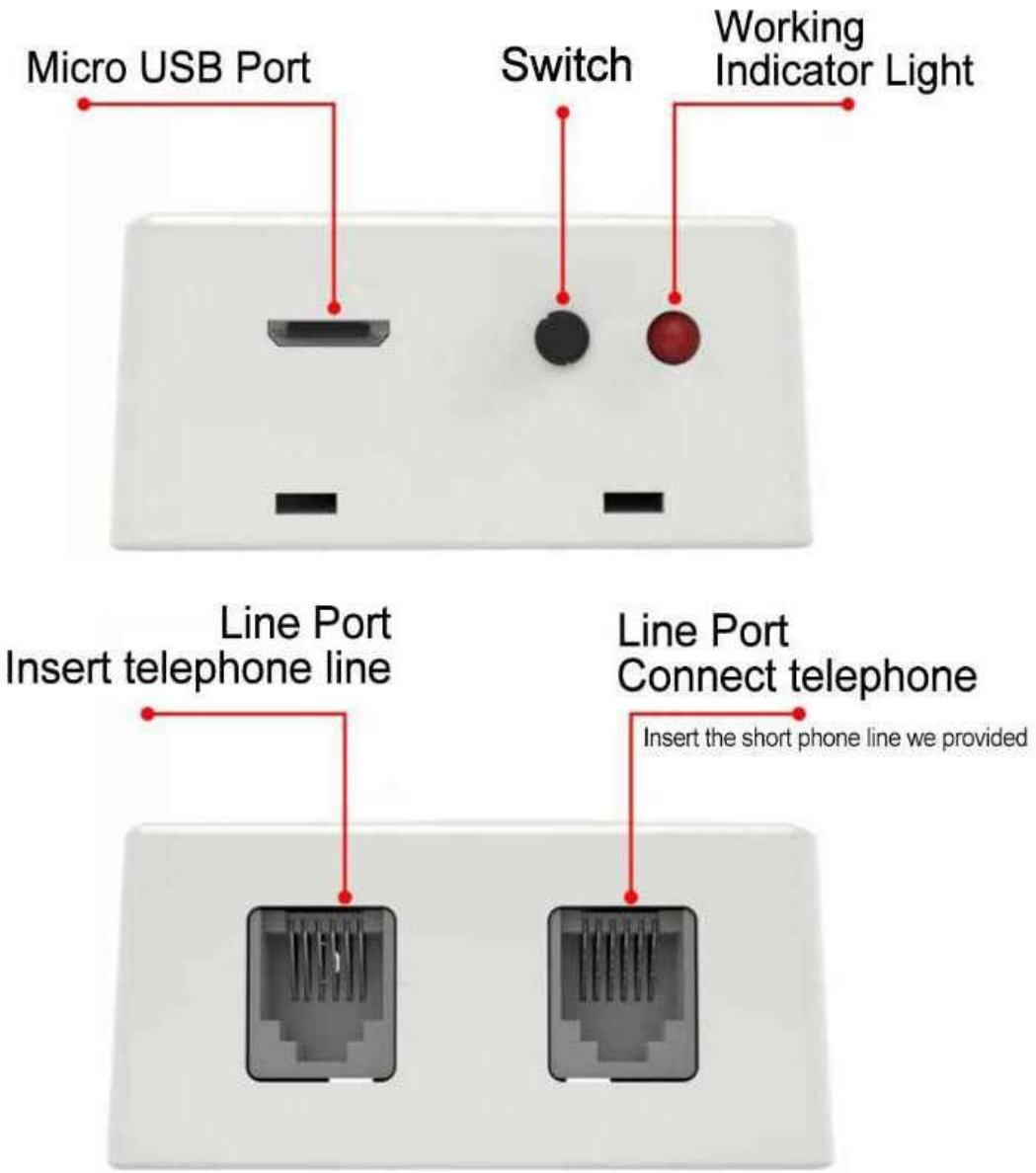


Примеры телефонных адаптеров.

Примеры телефонных адаптеров.

Примеры телефонных адаптеров.

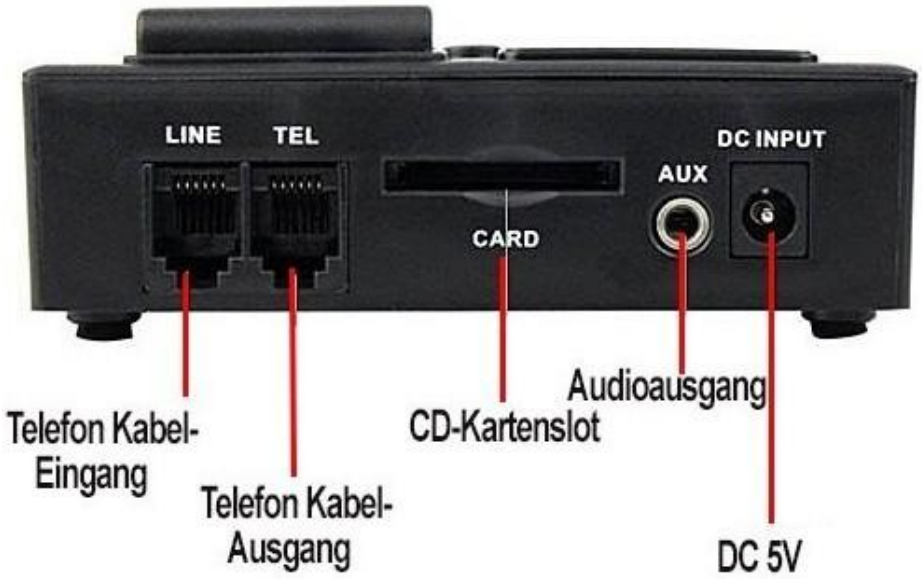
Пример телефонного адаптера с Bluetooth-соединением.



Принцип работы телефонного адаптера с Bluetooth-соединением.

Диктофон со встроенным телефонным адаптером.

1- Aufnahmeschalter
2- Abspielen
3- Automatische oder manuelle Aufnahmeschalter
4- Zeiteinstellung
5- Pause / Abspielen
6-LED-Anzeige
7- Lautstärke +
8- Bisherig
9- Nächster
10-Lautstärke -



Диктофон со встроенным телефонным адаптером.

Диктофон со встроенным телефонным адаптером.

ХАРАКТЕРИСТИКИ:

- 2 **режима** записи :
  - Автоматическая запись при ответе на звонок.
  - Ручной запуск нажатием кнопки.
- ЖК-дисплей с подсветкой с записью времени, даты и времени.
- Дополнительный выход для подключения наушников или внешних усилителей.
- **Сохраняет записи с отметкой времени.**
- Для работы от сети.
- Благодаря резервным батареям время и дата сохраняются, если источник питания отключен или происходит сбой питания.

Считывание записанных телефонных звонков:

- Вы извлекаете вставленную карту памяти и читаете ее на своем ПК или ноутбуке, либо слушаете записи прямо на устройстве. Для этого установлен динамик.

ТЕХНИЧЕСКИЕ ХАРАКТЕРИСТИКИ:

- Напряжение адаптера: AC110V 60 Гц / 220 В 50 Гц
- Мощность: DC 5 В 500 мА
- Подключение наушников: 3,5 мм
- Карта памяти: поддержка SD-карты до 8G (не входит в комплект)

Соединения:

- Соединительная телефонная линия
- Подключение телефона
- Aux - Гнездовой выход
- Слот для SD-карты
- Вес: 98 г
- Размер: 100x65x35 мм

Пример телефонного адаптера, подключаемого к линии ISDN.

ISDN Connection with Miniature Digital Recorder

The complete system consists of a tiny little transmitter and a miniature digital recorder. The transmitter can easily be installed into a telephone set or directly into the ISDN-line for a continuous monitoring and recording of both sides of telephone conversations via ISDN-lines. The full conversation will be recorded by the supplied digital recorder, which will only start when a telephone conversation begins. This saves storage capacity and provides a long-term recording. Each message automatically is date/time stamped by the built-in real-time clock and stored messages can be played back using an earphone or downloaded to a PC as standard sound files. Furthermore the recorder incorporates a high sensitively microphone, which covers a typical range of up to 8-10 meters.

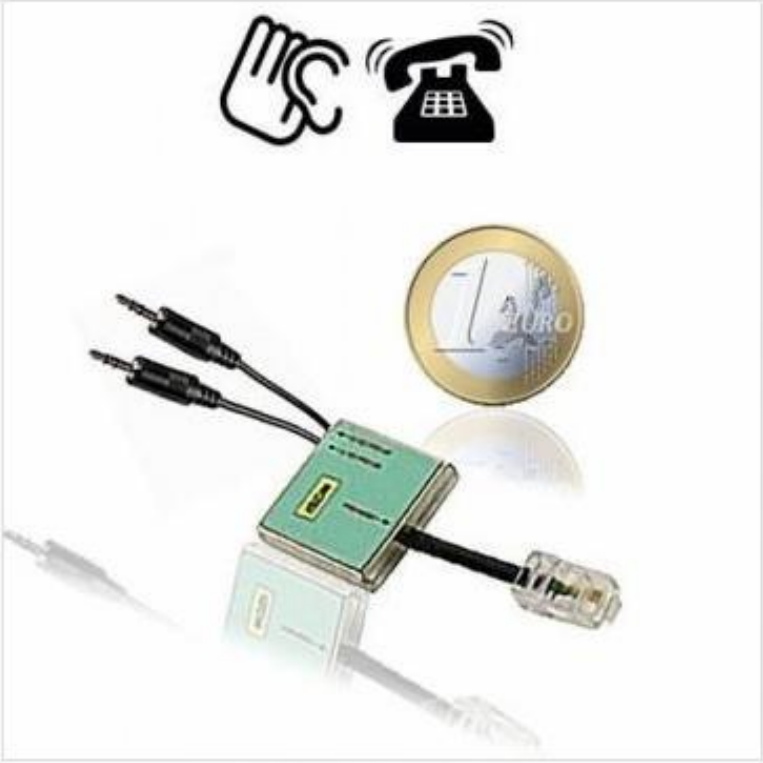
Specifications

- Professional connection to any ISDN- telephone system with automatic recording of conversations on digital recorder
- up to 140 hours recording time
- Automatic channel selection via jumper at S-bus of ISDN central
- Easy connection by supplied cables between S-Bus and recorder
- Digital recorder included
- VOX (voice control) of recorder is supported

http://www.pki-electronic.com/products/audio-surveillance-equipment/isdn-connection-with-miniature-digital-recorder

Пример телефонного адаптера, подключаемого к линии ISDN.

ISDN-Tonbandadapter, Basiskanal 1 + 2



ISDN Telefon Mitschnitt-Adapter

Top 1A HIGH-END Qualitäts-Produkt:

- Einziges Gerät auf dem Weltmarkt zum Direktanschluss am ISDN-Bus für simultanen Mittschnitt der ISDN-Basiskanäle 1 + 2.
- Glasklare Übertragung durch DVC
- **Jeder beliebige Voicerecorder anschließbar.**
- Ein einzigartiges und konkurrenzloses High-Tech Gerät.

PROFESSIONELLER ISDN RECORDER-ADAPTER ÜBERWACHT SIMULTAN BEIDE ISDN-KANÄLE.

Absolute Neuentwicklung. Der zur Zeit einzige ISDN-Tonband-Aufzeichnungsadapter der direkt über den RJ 45-Stecker am S0-Bus angeschlossen wird und gleichzeitig beide ISDN-Kanäle (Basiskanal 1 + 2) aufzeichnen kann. D.h. es ist nur ein ISDN-Adapter notwendig um alle ISDN-Telefonate zu überwachen, egal welche MSN genutzt wird. Es ist keine Batterie od. Netzteil notwendig, da das Gerät über den S0-Bus gespeist wird. Einfach in die ISDN-Anschlussdose einstecken und fertig !

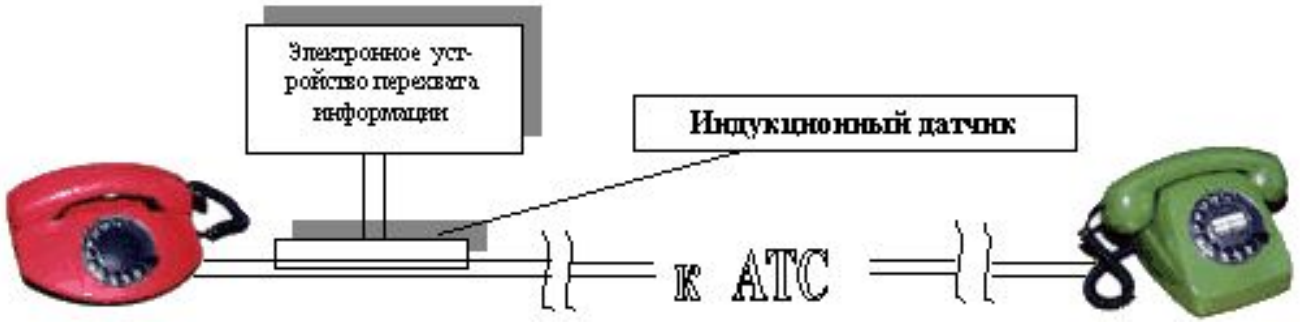
EIGENSCHAFTEN:

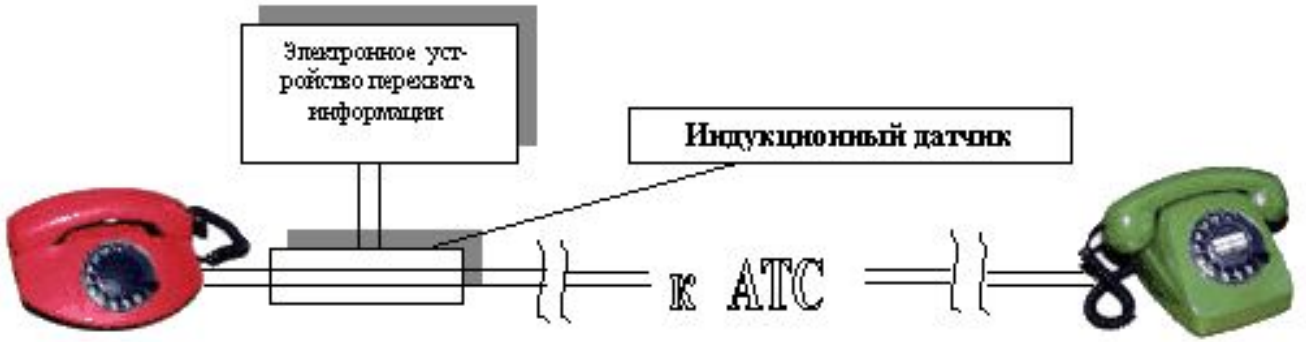
- Glasklare Übertragung durch DVC (Digital Voice Control) und AGC (Automatic Gain Control) von 20dB bis 120 dB.
- Jeder beliebige Voicerecorder anschließbar.
- Wir empfehlen unsere Digital-Voice-Recorder von 18 Std. bis zu 36 Stunden Aufzeichnungskapazität. (Siehe Zubehör).
- Ein einzigartiges und konkurrenzloses High-Tech Gerät.

https://www.spyshop-online.com/telefon-abhoergeraete/isdn-tonbandadapter.html

Вариант подключения через адаптер к VoIP сети.

Варианты бесконтактного (*индукционного*) подключения к телефонной линии.



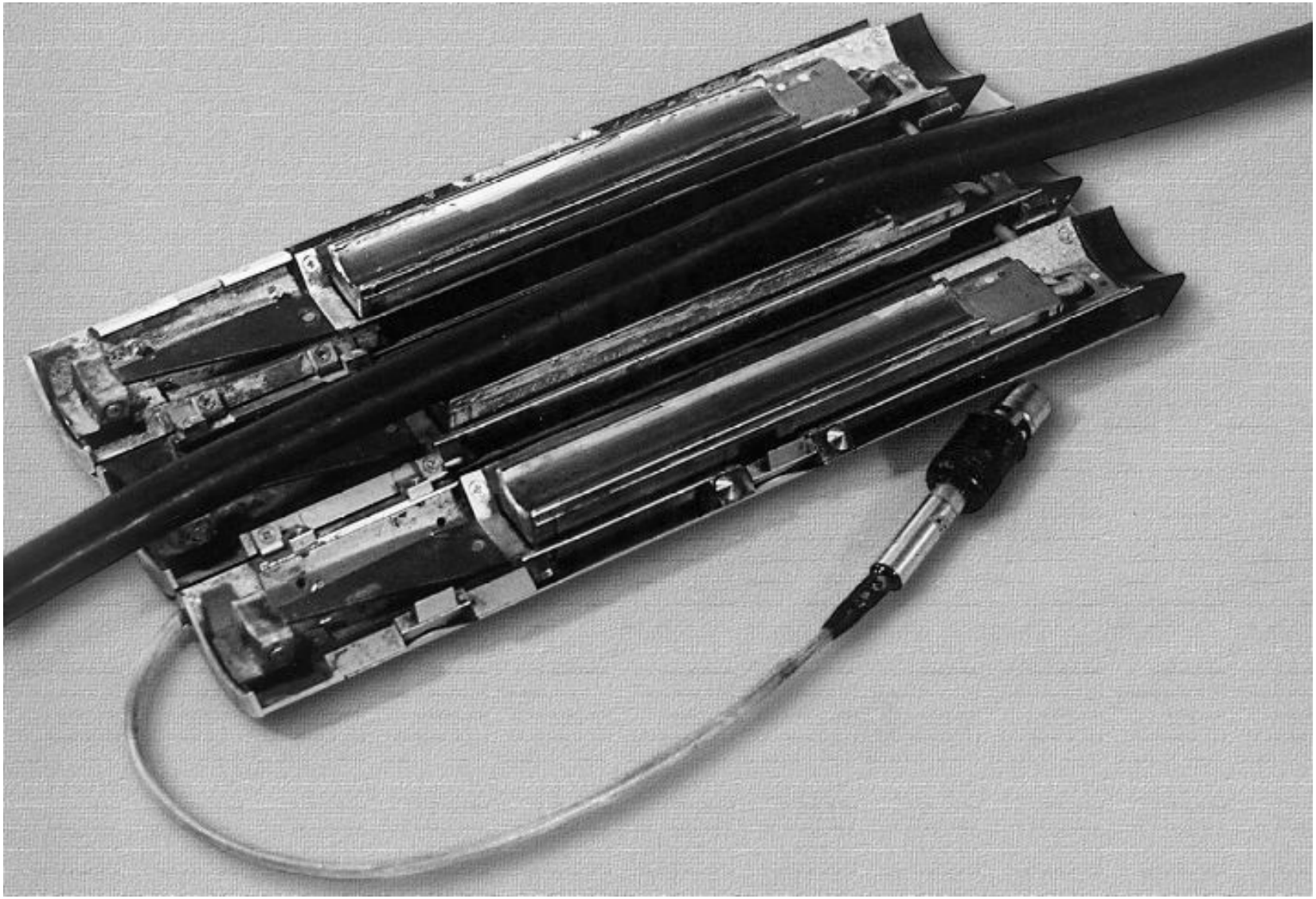


Хорев А.А. “Методы и средства защиты телефонных линий” / “Специальная техника”, 2001 г. № 2.

Примеры телефонных адаптеров с индукционным подключением.

Примеры телефонных адаптеров с индукционным подключением.

Примеры телефонных адаптеров с индукционным подключением.



Пример профессионального устройства контроля телефонных переговоров, использующего адаптер с индукционным подключением.

Telephone Tapping Device

The PKI 1860 can easily and quickly be installed on telephone lines, subject to entering the room at least once or for a short time. It allows continuous tapping of a telephone line without leaving outer traces. Just clip the contact clamp onto the telephone cable and listen to the conversation of both sides via the includedheadphones, or alternatively save it with a recording device.

Specifications

- The only way to tap telephone lines without having to cut them.
- Impossible to be detected or located via TDR reflectometer.
- Easy and quick installation – just fix the clamp onto the cable and turn it on.
- Equipped with connection sockets for headphones and recording device (D 1300)
- Dimensions: approx. 34 x 20 x 114 mm

http://www.pki-electronic.com/products/interception-and-monitoring-systems/telephone-tapping-device/

Системы записи телефонных переговоров.

В настоящее время системы записи телефонных переговоров широко распространены и активно используются во многих государственных и частных компаниях.

В то же время, необходимо помнить, что данные системы в руках злоумышленников могут выступать и в качестве мощного средства контроля телефонной сети – особенно учитывая тот факт, что большинство данных систем позволяет работать не только с аналоговыми, но и с цифровыми каналами связи (*фактически осуществляется “расшивка” стандартного цифрового сигнала*).

Назначение систем записи телефонных переговоров.

ДЛЯ ПРОДАЖ, МАРКЕТИНГА И СЕРВИСА

- Быстрое выявление и устранение слабых мест в подготовке сотрудников служб продаж и сервиса на основе данных системы записи телефонных разговоров.
- Грамотное разрешение спорных ситуаций с клиентами, поскольку все договоренности, сделанные по телефону, записаны.
- Анализ потребностей клиентов, озвучиваемых в телефонных разговорах с продавцами.
- Отслеживание эффективности рекламных компаний.
- Контроль интенсивности работы сотрудников путем получения отчетов из системы записи телефонных переговоров.

ДЛЯ ДИСПЕТЧЕРСКИХ СЛУЖБ

- Контроль и документирование действий диспетчеров.
- Выявление и устранение недостатков в работе диспетчеров.
- Получение информации о работе удаленных диспетчеров из одной точки.

ДЛЯ БАНКОВ

- Выявление слабых сторон в подготовке консультантов банка.
- Получение доказательной базы для разрешения споров.
- Выявление недобросовестных сотрудников, нарушающих коммерческую тайну.

ДЛЯ ОХРАННЫХ ПРЕДПРИЯТИЙ

- Контроль разговоров дежурной смены.
- Анализ и документирование действий сотрудников при внештатных ситуациях на объектах.
- Запись телефонных переговоров личного состава в процессе тренировок и учений, для выявления слабых сторон в подготовке.

https://agatrt.ru/zapis-telefonnyh-razgovorov/sprut-7-o-produkte/

Достоинства систем записи телефонных переговоров.

ДОСТУП К ЗАПИСАННЫМ РАЗГОВОРАМ ЧЕРЕЗ ИНТЕРНЕТ С ПОМОЩЬЮ МОБИЛЬНЫХ УСТРОЙСТВ

Для того, чтобы прослушать записанный телефонный разговор или увидеть статистику работы сотрудников по телефону, необязательно находиться в офисе за компьютером. Наличие доступа к сети Интернет позволяет обрабатывать записи удаленно, используя iPhone, iPad или другое мобильное устройство, оснащенное web-браузером.

ВОЗМОЖНОСТЬ ПОДКЛЮЧЕНИЯ И КОНТРОЛЯ ЛЮБЫХ ТЕЛЕФОННЫХ ЛИНИЙ

Система записи телефонных переговоров корректно работает с цифровыми (Up0, ISDN BRI, E1) и аналоговыми (FXS, FXO) каналами связи, IP-телефонией, подключается к линейным выходам микрофонов и радиостанций. Она позволяет контролировать все имеющиеся источники без необходимости использования дополнительного оборудования. Система записи переговоров совместима с цифровыми абонентскими линиями практически любых импортных УАТС, в частности: Alcatel, Avaya, Ericsson, LG, NEC, Coral, Panasonic, Siemens, Meridian, Samsung, Telrad и другие.

РАЗЛИЧНЫЕ ВАРИАНТЫ ИСПОЛНЕНИЯ СИСТЕМ ЗАПИСИ ТЕЛЕФОННЫХ ПЕРЕГОВОРОВ

В зависимости от задач и условий, в которых будет производиться контроль и запись телефонных переговоров, Вы можете выбрать наиболее оптимальный способ подключения контролируемых каналов к серверу записи. Предлагаемые варианты:

- платы PCI, PCI Express «Ольха-Р», встраиваемые в системный блок;
- сетевые регистраторы «Спрут NR» для автономного накопления информации;
- интеллектуальные серверы «Спрут SR» для записи в автономном режиме.

Использование автономного регистратора «Спрут NR» или интеллектуального сервера «Спрут SR» избавляет Вас от необходимости оснащения комплекса выделенным компьютером. В данном варианте, чтобы система записи телефонных переговоров «Спрут NR» или «Спрут SR» приступила к работе, достаточно просто подключить ее к телефонным линиям.

КОНТРОЛЬ УДАЛЕННЫХ ОФИСОВ

Уникальная архитектура программ-аппаратного комплекса записи телефонных переговоров «Спрут 7» позволяет создавать масштабируемые системы записи и контролировать от единиц до сотен каналов в рамках единой распределенной системы.

https://agatrt.ru/zapis-telefonnyh-razgovorov/sprut-7-o-produkte/

Пример системы записи телефонных переговоров “Спрут – 7”.

Аппаратно-программный комплекс, при помощи которого осуществляется автоматическая запись разговоров, как правило, состоит из ПО и адаптера подключения к линии. Он решает все базовые задачи записи телефонных разговоров, обладает широким сервисом, универсальностью и доступностью.

Как осуществляется запись телефонных переговоров

Телефонный регистратор с одной стороны подключается параллельно к контролируемым телефонным линиям и НЕ оказывает никакого влияния на работу Вашей телефонии. С другой стороны он сопрягается с компьютером-сервером записи через шину PCI, PCI Express, интерфейсы USB или LAN. На этот же компьютер-сервер устанавливается система записи телефонных переговоров «Спрут-7».

После окончания установки ПО производится несложная настройка автоматической записи телефонных разговоров, задаются правила хранения записанной информации – оборудование готово к работе.

Система записи переговоров с телефонных линий «Спрут-7» в автоматическом режиме фиксирует подробную информацию о каждом телефонном разговоре:

- Дата.
- Время.
- Продолжительность звонка.
- Номер вызывающего абонента.
- АОН и так далее.

Для удобства пользователей система записи телефонных переговоров на компьютер «Спрут-7» предусматривает возможность контроля телефонных линий в реальном времени, ведения статистики, построения отчетов по записанным разговорам и обработки записанных данных при помощи специализированного ПО или через WEB.

https://agatrt.ru/zapis-telefonnyh-razgovorov/sprut-7-o-produkte/

Примеры аналоговых систем записи телефонных переговоров “SELENA”.

Плата записи 2-х каналов с аналоговых линейных входов (микрофонов) или телефонных линий под PCI слот ПК со встроенными активным и пассивным определителями номера. **Плата обеспечивает одновременное подключение 2 телефонных линий и 2 микрофонов. Переключение между источниками сигнала осуществляется программно, что позволяет вести поочередную запись с разных типов источников.**

Отличительные особенности:

- возможность подключения двухпроводных микрофонов с фантомным питанием от платы;
- возможность плавной регулировки чувствительности каждого канала;
- возможность объединения моно входов в стерео;
- программно-аппаратное сжатие по алгоритму MPEG-3;
- программное переключение телефонных и микрофонных входов (комплексный канал);
- 2 дополнительных alarm- входа для подключения различных датчиков;
- автоматическое измерение уровня входных сигналов и состояния телефонных линий;
- самодиагностика и контроль работоспособности платы;
- программно - аппаратный формирователь сигнала “запрос пакета АОН”;
- автоматическое определение наличия сигнала “ВЫЗОВ”;
- автоматическое определение и дешифровка факсимильных сообщений (при установленном программном модуле SEL FAX);
- полная гальваническая развязка входов.

https://suritel.ru/catalog/our-products/multichannel-audiologging-system-selena-np/

Примеры систем записи телефонных переговоров “SELENA”.

Внешнее сетевое устройство записи информации с 4 цифровых абонентских линий, подключаемое к компьютеру через сетевой порт и взаимодействующее с ним по протоколу TCP/IP.

Отличительные особенности:

- полный анализ и декодирование D-канала;
- параллельное подключение к линиям;
- оптическая развязка с линиями;
- поддержка баз данных формата MS SQL;
- индикация настройки синхронизации каналов.

Комплект поставки:

- Устройство SEL DSR NET - 4;
- Программное обеспечение.

https://suritel.ru/catalog/our-products/multichannel-audiologging-system-selena-np/

Примеры систем записи телефонных переговоров “SELENA”.

Внешнее сетевое устройство записи информации 1 цифрового потока E1 (30 каналов), подключаемое к компьютеру через сетевой порт и взаимодействующее с ним по протоколу TCP/IP.

Отличительные особенности:

- полный анализ и декодирование D-канала;
- параллельное подключение к линиям;
- возможность использования совместно с удлинителем-ответвителем потоков E1 SEL COUPLER для подключения к линиям на расстоянии до 300 м (Удлинитель-разветвитель цифровых потоков SEL COUPLER подключается к модулю SEL DSR NET - E только с внешним источником питания);
- оптическая развязка с линиями;
- автоматическое определение и дешифровка факсимильных сообщений (при установленном программном модуле SEL FAX);
- поддержка баз данных формата MS SQL.

https://suritel.ru/catalog/our-products/multichannel-audiologging-system-selena-np/

Пример системы мониторинга цифровых линий связи (ISDN).

PC-supported Telephone Monitoring System

The surveillance of any kind of telecommunication, of course, is our main field of business. Whether analogue, digital or cellular, you will find the corresponding monitoring device in our scope of supply and in this catalogue. The PKI 1850 has been developed for the monitoring of digital and ISDN telephone lines. But the main advantage is that it can be used for stationary and mobile use. Without any problem each necessary data, like telephone number, date, time and other criteria can be stored on a laptop. Each call will be stored as a WAV-file. By means of the supplied software, the WAV-file can easily be administrated and can be opened to hear the content of each call plus indicating the relevant data. Each WAV-file can be stored in compressed or uncompressed version for further action.

Specifications

- Dimensions of unit without laptop approx. 76 x 55 x 19 mm
- Weight of unit without laptop approx. 50 g
- SO-interface ITU-Standard I.430
- Connection 2 x RJ45 Western Modular
- Tests Polarity, Framing, Power, Protocol
- Channels 2 x (D, B1, B2), E, M, A, Q, S • USB 1.1 and 2.0 (full speed)
- USB socket USB Type B
- Power < 90 mA
- LEDs 4 x red/green
- Storage: 16 KB per second/call, uncompressed WAV file.
- Sampling frequency 8000 Hz
- WAV format A-Law Stereo, Mono, MP3, GSM
- Operating System required on PC/laptop: Windows 2000, Windows Server 2003, Windows XP, Windows Vista
- Software disk space max. 140 MB
- Processor 500 MHz (min for single device operation)
- Connection to telephone system Point-to-Point or Point-to-Multipoint
- Device package includes
- PKI 1850 device, Software-CD, USB and ISDN cables, instruction manual

http://www.pki-electronic.com/products/interception-and-monitoring-systems/pc-supported-telephone-monitoring-system/

Пример системы мониторинга, позволяющей контролировать VoIP .

IP Monitoring System

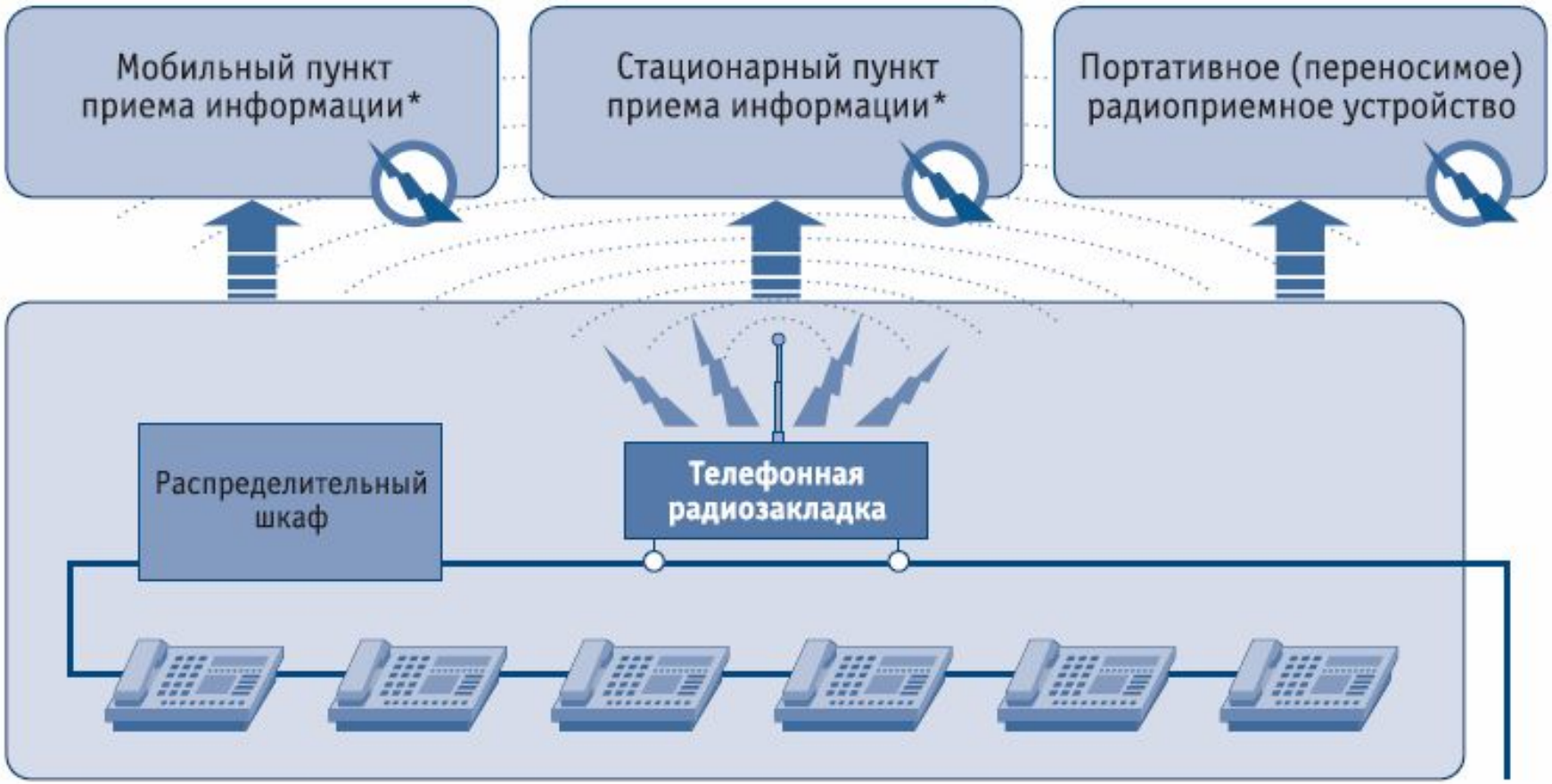
Specifications

- Monitoring of up to 4 networks simultaneously
- Data storage on internal HDD up to 5 TB
- Protocols: ARP, FTP, Gopher, HTTP, SMTP, POP, Telnet, ICMP, IP, VOIP ...
- Connections: LAN 4 x for repeater 1 x for WAN
- Repeater: LAN or connection via tapping module directly to a telephone or ISDN line. WLAN receiver.
- Operating voltage: 230 V
- Housing: 19 inch 3 RU

The technologies applied for communication have increasingly shifted into the IP sector. Whether e-mail, telephone (VOIP), fax, etc.: today, all these means of communication demand digital bandwidth and are transmitted via IP-based networks. In contrast to the technologies applied so far, with IP technology no direct connection is established between the communication partners but communication is digitized, packed in small packets, possibly encrypted and subsequently more or less quickly and frequently exchanged. In case of previous monitoring systems, a known sender automatically meant that the receiver was known, too. The conversation, fax, etc. was realized via a line to which both participants were connected. The data volume recorded this way is and remained manageable. The problem with today´s IP-based technology is that there is no direct connection any longer but only a communication distributed onto numerous packets. It is therefore necessary to separate the corresponding packets from the entire mass of data and to merge and decode them subsequently. Such a system shall in fact record the ongoing data traffic but it can not participate actively. What is difficult are e.g. lost packets which can not be requested again or also packets transmitted several times in order to put together the original message. The solution to this is our PKI 1100 IP Monitoring System. Integrated into the network to be monitored, any communication is stored and decoded to the greatest possible extent. And it is irrelevant whether a WLAN or a wired network is eavesdropped on here. The actual access to the network is realized with a repeater establishing the connection to the PKI 1100. The system logs all captured data into a database and thus enables a subsequent evaluation. Via the IP address, an assignment is then possible, via the data of the providers, to the user identity.

http://www.pki-electronic.com/products/interception-and-monitoring-systems/ip-monitoring-system/

Перехват информации, передаваемой по телефонной линии связи, с использованием телефонных радиозакладок.



** Оборудование премного пункта: наушники, радиоприемное устройство, магнитофон*

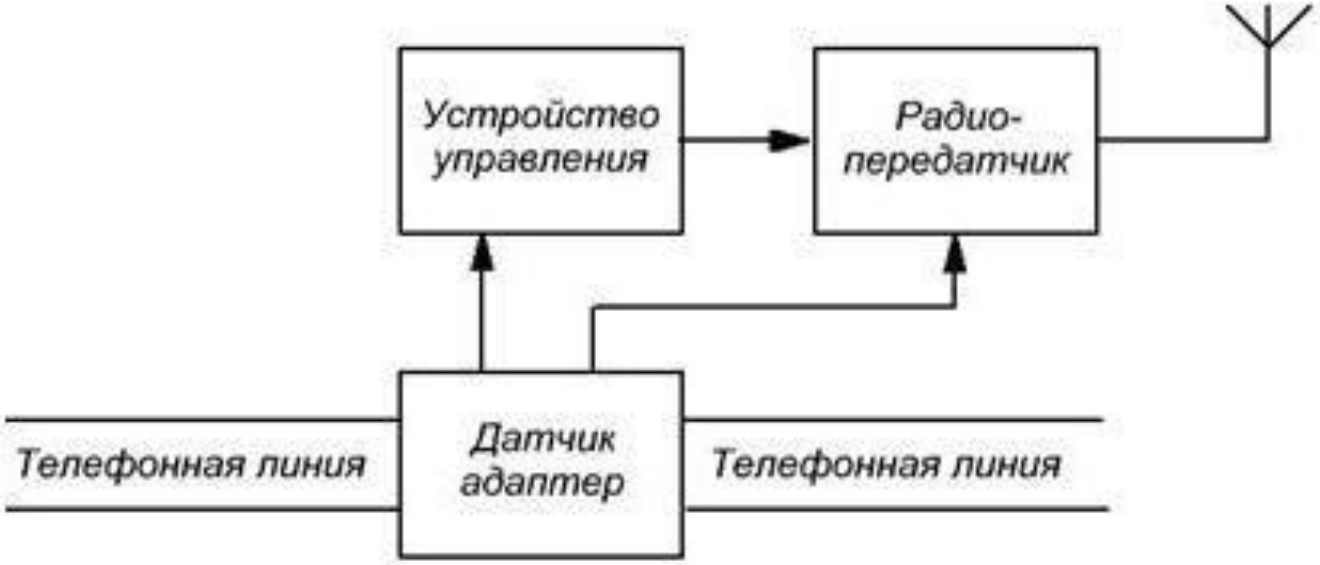
Хорев А.А. Техническая защита информации: учеб. пособие для студентов вузов. В 3 т. Т. 1. Технические каналы утечки информации. − М.: ООО «НПЦ Аналитика», 2008.

Классификация электронных устройств перехвата информации с проводных линий связи (*телефонных закладок*).

Показатель классификации	Значения
Вид датчика	1. Телефонный адаптер. 2. Магнитная антенна.
Способ подключения к линии	1. Последовательное (в разрыв одного провода). 2. Через индукционный датчик (без нарушения целостности проводов линии). 3. Параллельное (без разрыва линии).
Место установки	1. В корпусе телефонного аппарата или телефонной трубки. 2. В телефонной розетке. 3. В телефонной линии.
Способ передачи информации	1. По радиоканалу. 2. По другой незанятой телефонной линии.
Тип источника питания	1. От телефонной линии. 2. От автономных источников питания.
Вид исполнения	1. Обычные (отдельные модули). 2. Камуфлированные (в виде телефонной розетки, конденсатора, микротелефонного капсюля и т.п.).
Способ управления передатчика	1. Неуправляемые (с включением передатчика при снятии трубки телефонного аппарата). 2. Дистанционно управляемые.
Способ накопления информации	1. Без накопления. 2. С промежуточным накоплением (с коротким и длительным временем накопления).
Способ кодирования информации	1. Без кодирования информации. 2. С аналоговым скремблированием сигнала. 3. С цифровым шифрованием информации.
Вид используемых сигналов	1. Простые аналоговые сигналы (AM, NFM, WFM модуляция). 2. Цифровые сигналы с частотной модуляцией (FSK, FFSK, GMSK). 3. Сложные шумоподобные сигналы с фазовой модуляцией (PSK, BPSK,QPSK). 4. Сигналы с псевдослучайной перестройкой несущей частоты (ППРЧ).

Хорев А.А. Техническая защита информации: учеб. пособие для студентов вузов. В 3 т. Т. 1. Технические каналы утечки информации. − М.: ООО «НПЦ Аналитика», 2008.

Структурная схема телефонной радиозакладки (*телефонного радиоретранслятора*).



Габариты телефонных радиозакладок могут быть минимальными – например, в виде типового конденсатора.

В первую очередь это связано с наличием “готового” электропитания (*напрямую от телефонной линии*) и использованием телефонной линии в качестве антенны.

Возможные схемы подключения телефонных радиозакладок к телефонной линии.

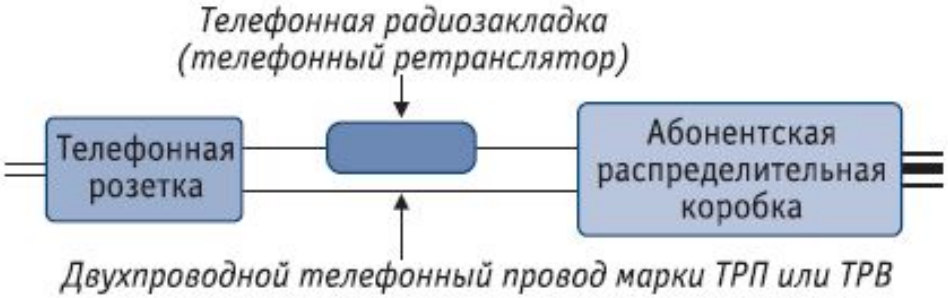


Схема последовательного подключения закладного устройства к телефонной линии

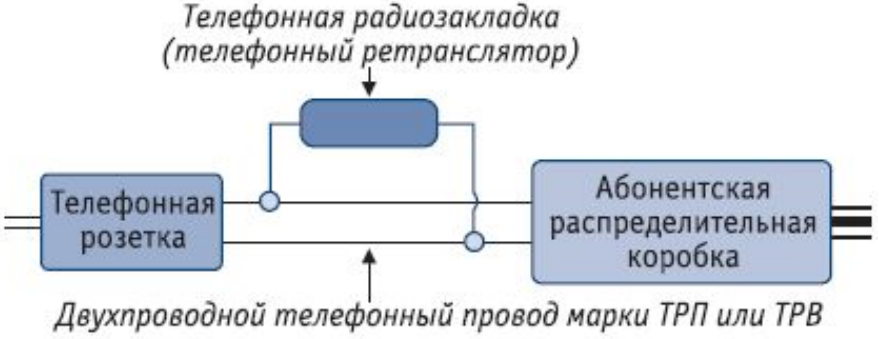


Схема параллельного подключения телефонной закладки к абонентской проводке (питание от телефонной линии)

Хорев А.А. Техническая защита информации: учеб. пособие для студентов вузов. В 3 т. Т. 1. Технические каналы утечки информации. − М.: ООО «НПЦ Аналитика», 2008.

Возможные схемы подключения телефонных радиозакладок к телефонной линии.

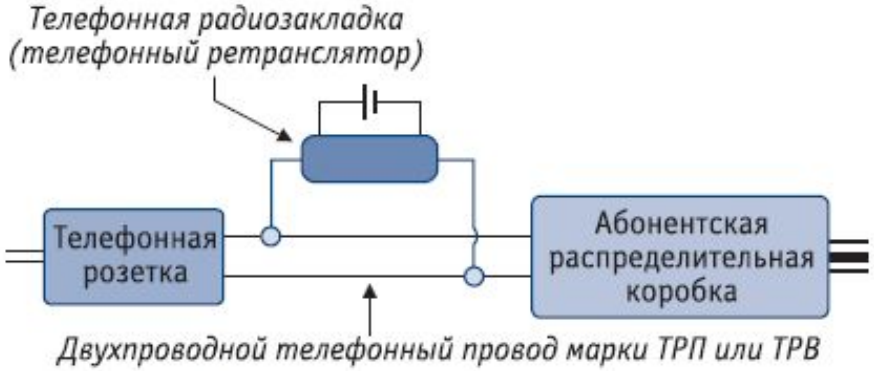


Схема параллельного подключения телефонной закладки к абонентской проводке (с питанием от автономного источника питания)

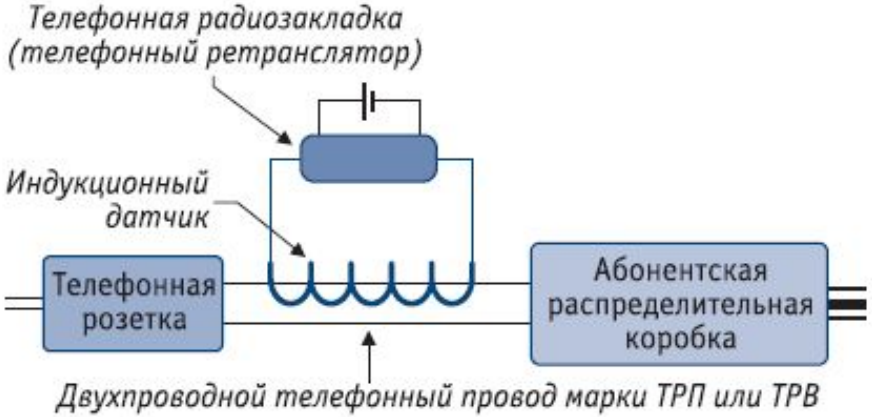
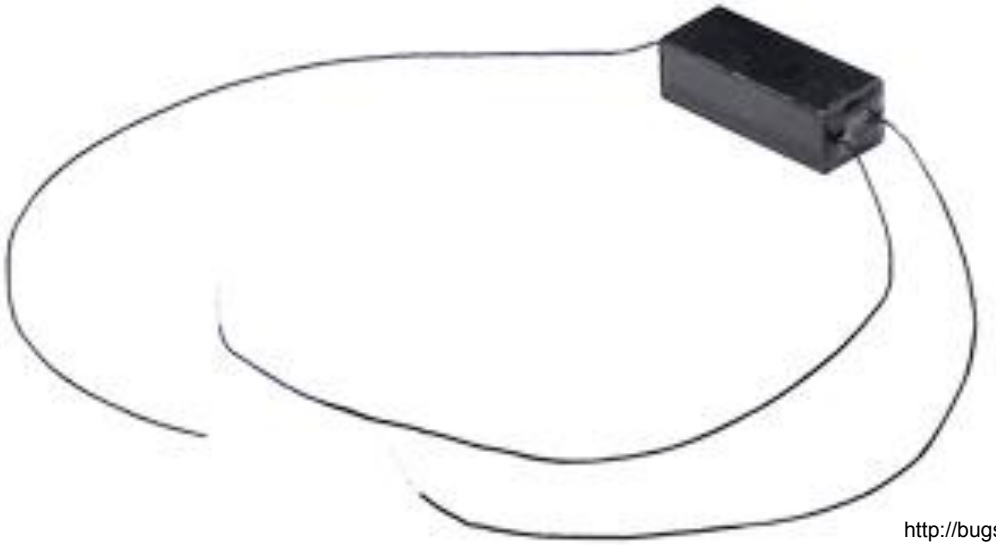


Схема подключения закладного устройства к телефонной линии с использованием индукционного датчика (бесконтактное подключение)

Хорев А.А. Техническая защита информации: учеб. пособие для студентов вузов. В 3 т. Т. 1. Технические каналы утечки информации. − М.: ООО «НПЦ Аналитика», 2008.

Некоторые возможные места установки телефонных радиозакладок.

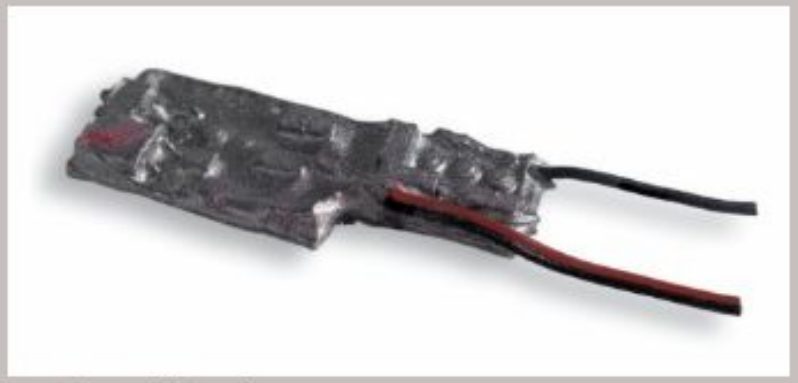
Примеры профессиональных телефонных радиозакладок.



http://bugspy.narod.ru/index.files/stran/Spetstechnika/telobsh.html

Пример профессиональной телефонной радиозакладки.

Telephone Transmitter (PCB)



In many cases of observation the telephone conversations have to be monitored. With the PKI 2270 such tasks can easily be done. Due to its small size and unobtrusive appearance, this transmitter really is the champion in its class. The transmitter is supplied as a printed circuit board (PCB) only and is coated with a special protective lacquer which protects it against environmental conditions. This allows a fast and easy installation into every kind of analogue telephone set in which it looks like a standard component being completelyinconspicuous to the user. The installation inside the telephone set should be made in serial mode; both polarities are allowed. PKI 2270 is only transmitting when a telephone conversation starts and therefore is non-detectable when the telephone is not in use. Another advantage is the independence from short-lived power supplies like batteries as the unit is continuously powered from the telephone line.

Specifications

- Easy to disguise
- Looks like installed standard components
- Automatic off-hook detection
- Long term unattended operation
- Quick installation
- UHF frequency around 427 MHz
- Crystal controlled
- 5 mW output power
- Antenna via telephone cable
- Serial mode connection
- Both polarities allowed
- Dimensions 30x14x7 mm

http://www.pki-electronic.com/products/audio-surveillance-equipment/telephone-transmitter-pcb/

Пример профессиональной телефонной радиозакладки.

Telephone Transmitter

If a telephone monitoring operation is on long term basis or access to the target area is restricted then the PKI 2210 Telephone Transmitter is the perfect solution. It is not necessary to have direct access to the telephone set. Any location along the telephone line can be used for monitoring. This transmitter operates automatically, i.e. the internal off-hook detection circuit automatically switches from standby to activation and transmission. Only transmitting when a telephone conversation takes place, this wireless bug is undetectable. The sensitivity on the telephone line can be adjusted manually. Another advantage is its independence from short-lived power supplies like batteries, so that a continuous monitoring of the target area is guaranteed. The installation on the telephone line should be made in serial mode. Both polarities are allowed. PKI 2210 is available in standard UHF. Special frequencies on request.

Specifications

- Quick and easy installation
- Designed for professional use
- Automatic off hook on telephone lines
- Ideal for long term, unattended operation
- Smallest dimensions
- Unlimited operation time
- 5 mW output power
- UHF frequency
- External antenna
- Dimensions: 24x14x8 mm

http://www.pki-electronic.com/products/audio-surveillance-equipment/telephone-transmitter/

Пример профессиональной телефонной радиозакладки, подключаемой к линии ISDN.

ISDN-S-Bus Telephone Transmitter / Receiver

The complete system, consisting of transmitter and receiver, is to be used especially for ISDNBus telephones with a direct connection to S-Bus of NTBA. Each part of the system features small size, robust metal housing and easy handling. The minimised size of the transmitter allows an easy installation into the junction box at NTBA SBus. ISDN channel selection provided by a jumper and the high output power of approx. 20 mW is the guarantee for a transmitting distance of at least several hundred meters. Under good surrounding conditions even one kilometer or more is possible. The receiver is equipped with connection for any digital recorder.

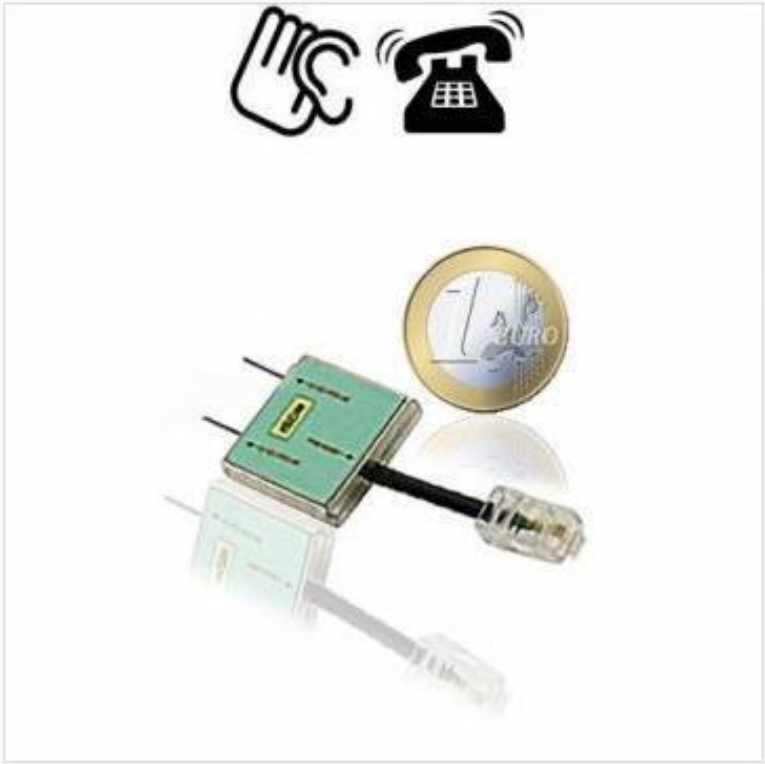
Specifications

- For direct connection to S-Bus of NTBA
- Wireless transmission of all conversations to supplied receiver
- ISDN channel selection by jumper
- Battery operated receiver with dimensions 55x25x112 mm
- Transmitter's power supply by NTBA
- 20 mW output power at around 418 or 433 MHz
- Dimensions 65x35x15 mm

http://www.pki-electronic.com/products/audio-surveillance-equipment/isdn-s-bus-telephone-transmitter-receiver/

Пример профессиональной телефонной радиозакладки, подключаемой к линии ISDN.

2-Kanal ISDN-Telefonsender



Top 1A HIGH-END Qualitäts-Produkt:

- Einziges Gerät auf dem Weltmarkt zum Direktanschluss am S0-Bus, mit simultaner Überwachung der ISDN Basiskanäle 1 + 2
- **10 mW HF-Out** (Sendeleistung).
- **Bis 1000 mtr. (**Relative Reichweite).

PROFESSIONELLER ISDN-TELEFONSENDER, ÜBERWACHT SIMULTAN BEIDE ISDN-KANÄLE

Absolute Neuentwicklung. Der zur Zeit einzige echte ISDN-Telefonsender der direkt über den RJ 45-Stecker am S0-Bus angeschlossen werden kann und der gleichzeitig beide ISDN-Kanäle (Basiskanal 1 + 2) überwacht. D.h. es ist nur ein einziges Gerät notwendig um alle ISDN-Telefonate zu überwachen, egal welche MSN genutzt wird.

EIGENSCHAFTEN:

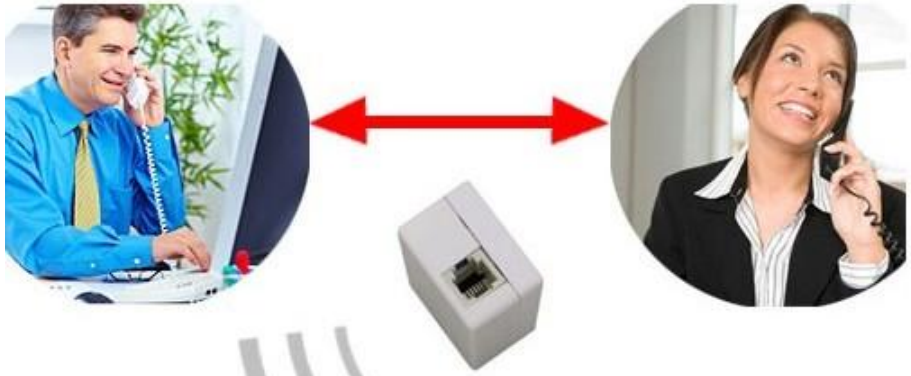
- **Relative Reichweite bis 1000 mtr..**
- Es ist keine Batterie od. Netzteil notwendig, da das Gerät über den S0-Bus gespeist wird.
- **Einfach in die ISDN-Anschlussdose einstecken und fertig !**
- Glasklare Übertragung durch DVC (Digital Voice Control) und AGC (Automatic Gain Control) von 20dB bis 120 dB.
- Ein einzigartiges und konkurrenzloses High-Tech Gerät.

LIEFERUMFANG:

1x ISDN Telefonsender

https://www.spyshop-online.com/telefon-abhoergeraete/isdn-phonetransmitter.html

Пример телефонной радиозакладки с передачей информации по сети GSM.



Telefonate mithören grenzenlos, weltweit !

Und so funktioniert‘s !

Телефонная радиозакладка с передачей информации по сети GSM.

TELEFON FERN-ABHÖRGERÄT MIT SIMULTNER WEITERLEITUNG AUF IHR HANDY.

Dieses Telefon-Abhörgerät wird mit wenigen Handgriffen einfach zwischen Ihr Telefon und die Telefonbuchse gesteckt und ermöglich eine **Live-Telefonüberwachung ohne Limits**. Ganz gleich wo Sie sich auch geographisch befinden.

Zusätzlich werden die Gespräche auch noch auf einer Speicherkarte (Micro-SD) im Gerät mitgeschnitten.

Sie kommen damit in die Lage jederzeit den in Frage kommenden Telefonanschluss umfassend zu kontrollieren, sofort und gleich, also in Echtzeit . Das bietet Ihnen dann auch die Möglichkeit sofort und ohne Zeitverlust mit der von Ihnen gewünschte Massnahme reagieren oder einzugreifen.

Das Gerät kann so eingestellt werden, dass Sie bei Beginn eines Telefonates auf Ihrem Handy oder Festanschluss angerufen werden und Sie sich dann sofort live und unbemerkt mitten im Dialog der beiden Gesprächsteilnehme befinden.

Sollte der Rufaufbaueinmal scheitern, weil Sie nicht erreichbar sind, wird das Gespräch mitgeschnitten.

Auf diese Art entgeht Ihnen garantiert nichts mehr.

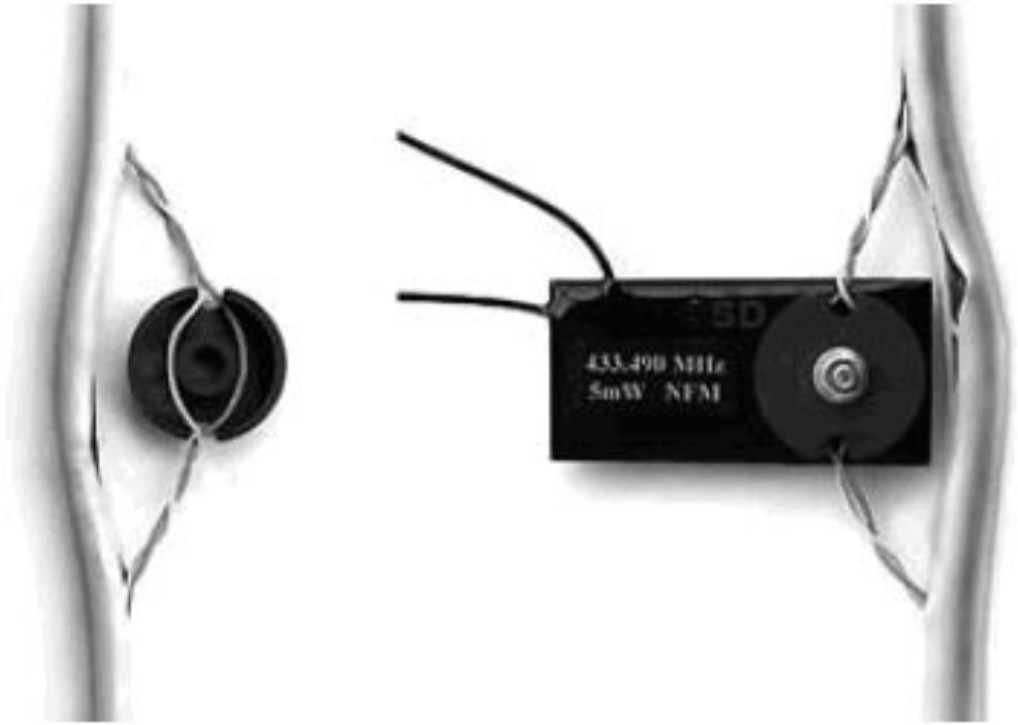
Nicht für atypische Telefonanschlüsse wie ISDN od. VOIP geeignet.

TECHNISCHE DATEN:
- Festnetz Gesprächstransponder mittel GSM.
- SIM-Karten-Slot (Normalgrösse).
- SD-Karten-Slot.
- RJ11 Anschlussbuchsen für Line-In/Line-Out
- Für analoge Telefone (kein ISDN od. VOIP).
- Eingebauter Akku - Dauerbetrieb bis zu 6 Monate.
- Abmessungen: 59mm * 36mm * 25mm.

LIEFERUMFANG:
1x Telefon-Abhörgerät Komplett
1xBedienungsanleitung

https://www.spyshop-online.com/festnetz-abhoergeraete/telefon-fernabhoersender.html

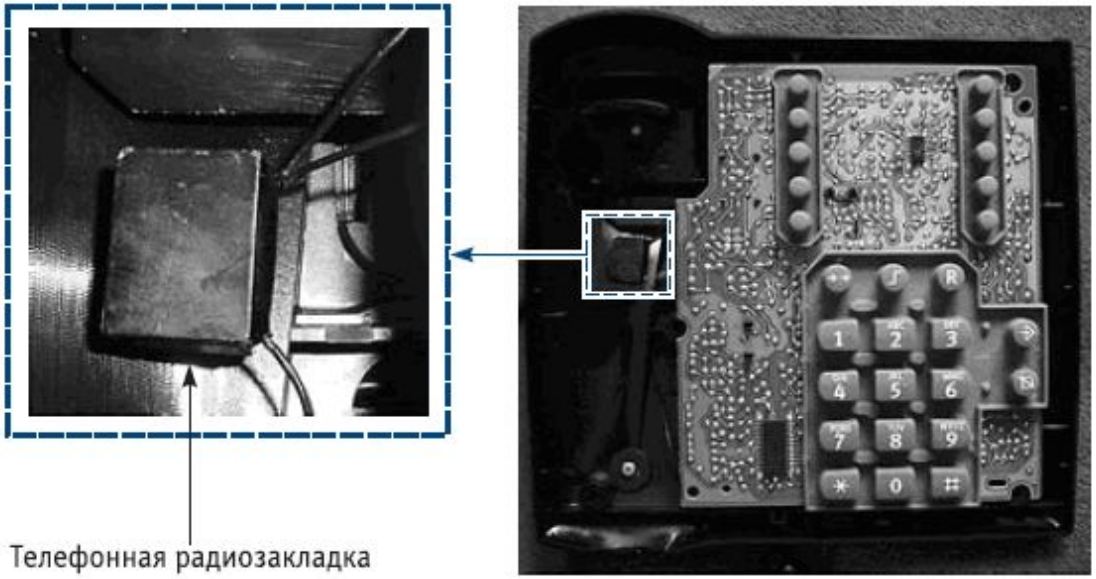
Пример телефонной радиозакладки, подключённой к телефонной линии с использованием индукционного датчика.



Хорев А.А. Техническая защита информации: учеб. пособие для студентов вузов. В 3 т. Т. 1. Технические каналы утечки информации. − М.: ООО «НПЦ Аналитика», 2008.

Примеры телефонных радиозакладок, установленных в абонентском оборудовании.

Телефонная радиозакладка, установленная в трубке телефонного аппарата



Телефонная радиозакладка, установленная в корпусе телефонного аппарата

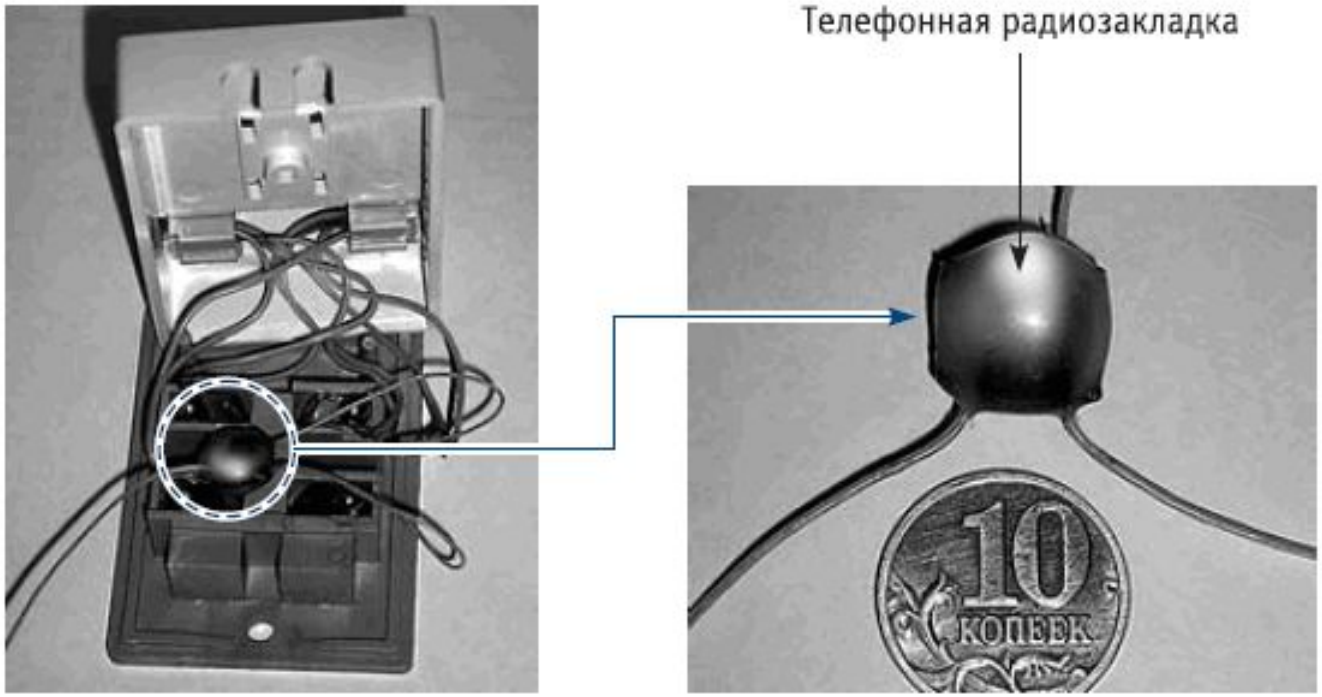
Хорев А.А. Техническая защита информации: учеб. пособие для студентов вузов. В 3 т. Т. 1. Технические каналы утечки информации. − М.: ООО «НПЦ Аналитика», 2008.

Пример телефонной радиозакладки, установленной в абонентском оборудовании.

Примеры телефонных радиозакладок, установленных в абонентском оборудовании.

Хорев А.А. Техническая защита информации: учеб. пособие для студентов вузов. В 3 т.
Т. 1. Технические каналы утечки информации. − М.: ООО «НПЦ Аналитика», 2008.

Пример телефонной радиозакладки, подключённой на участке абонентской линии.



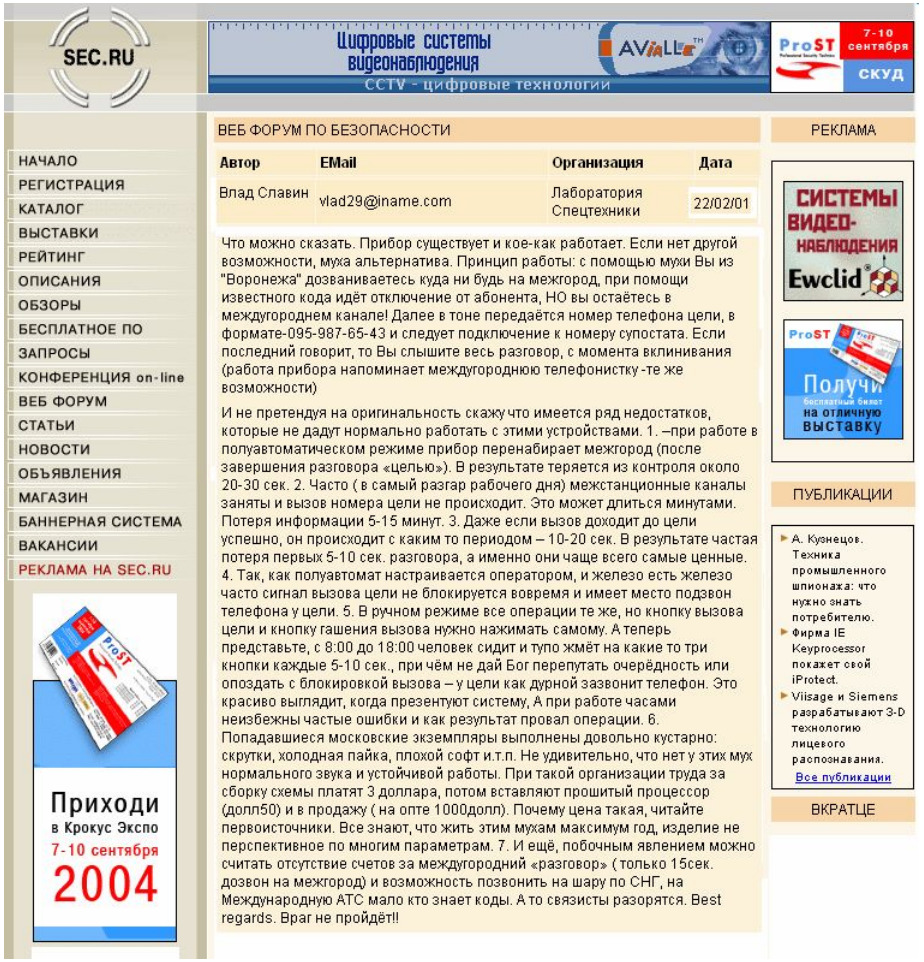
Телефонная радиозакладка, установленная в телефонной розетке

Хорев А.А. Техническая защита информации: учеб. пособие для студентов вузов. В 3 т. Т. 1. Технические каналы утечки информации. − М.: ООО «НПЦ Аналитика», 2008.

Один из вариантов классификации электронных устройств перехвата информации с проводных линий связи (телефонных закладок).

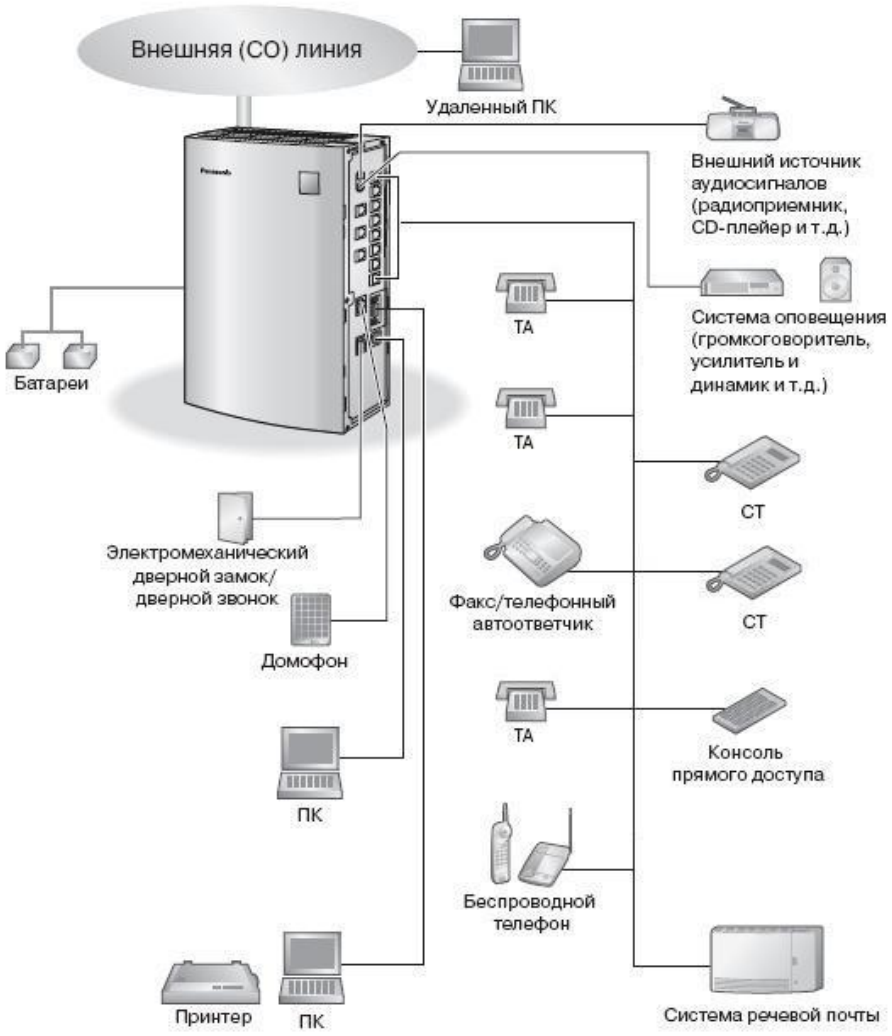
Хорев А.А. “Технические каналы утечки информации, передаваемой по каналам связи” / “Специальная техника”, 2004 г. № 6.

Изделия типа “FLY” (*когда-то было и такое – см. год*).



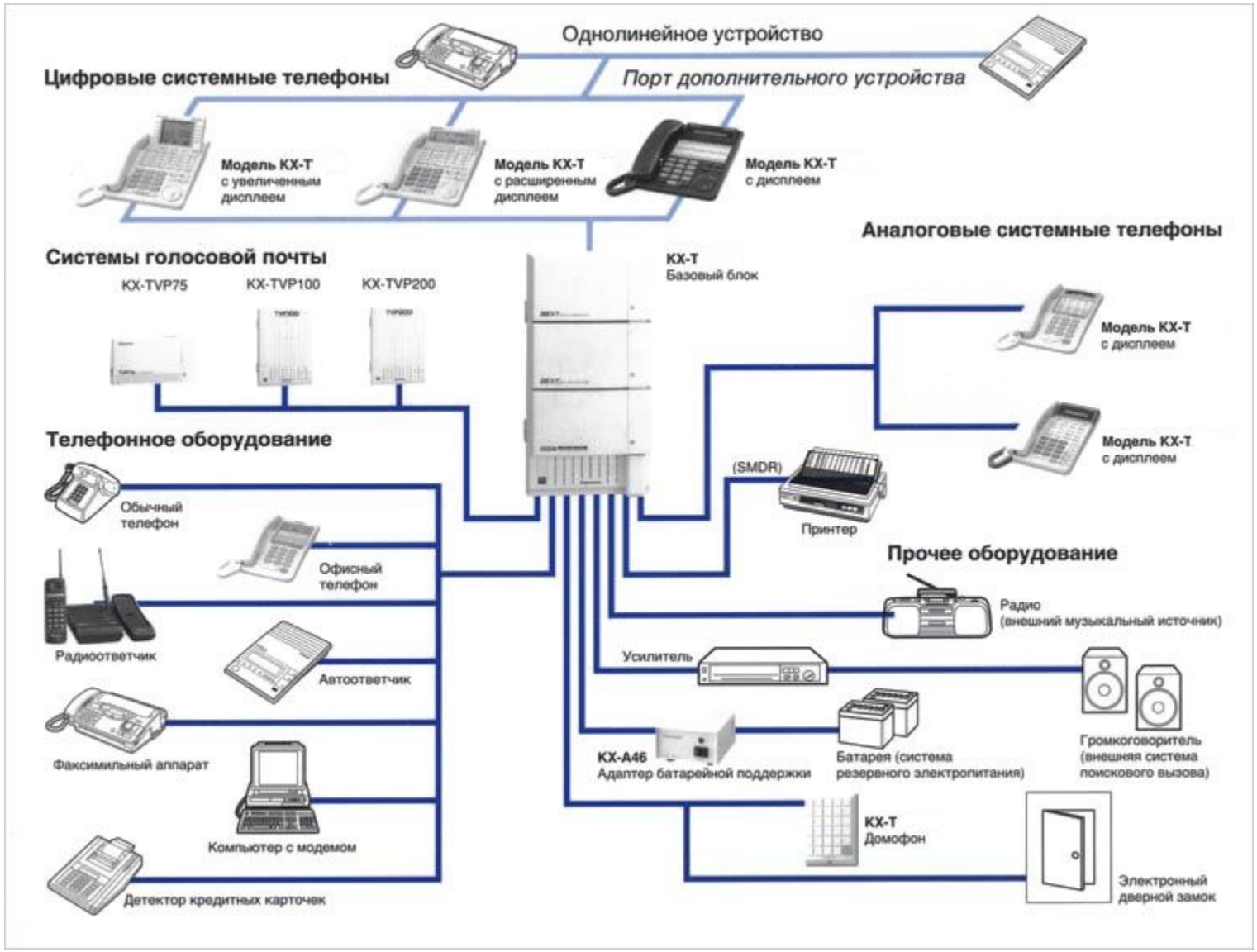
http://www.sec.ru/forum2.cfm?posa=2&stpa=10&threadid=283&read=1&stp=20&pos=1&

Прослушивание телефонных переговоров, осуществляемое за счёт “дополнительных” функций АТС.



- Большинство современных мини-АТС позволяют осуществлять скрытый контроль (прослушивание в режиме реального времени или запись) ведущихся по ним телефонных переговоров.
- Данная возможность реализуется за счёт функции “**Вторжение в разговор**” и функции “**Автоматическая запись в систему голосовой почты**” – после соответствующей предварительной настройки (программирования) АТС. Так же возможны различные варианты, связанные с **режимом “конференц-связи”**.
- Ещё раз хочу отметить, что данные функции являются **именно “дополнительными”** – *не путать с “не декларированными возможностями” телекоммуникационного оборудования* – т.е. они чётко прописаны в “Руководстве пользователя” и не являются “секретными”. Другое дело, что большинство “пользователей” в лучшем случае читают только первые две-три страницы “Руководства…” и, естественно, находятся “не в курсе дела” по данному вопросу.

Типовая схема офисной мини-АТС, в которой используются “системные” телефоны и “система голосовой” почты.



Прослушивание телефонных переговоров, осуществляемое за счёт функции “Вторжение в разговор”.

Данная функция позволяет “вклиниваться” с “системного” телефона в разговор, который ведётся по другому телефону, подключённому к мини-АТС.
С помощью программирования АТС можно выбрать различные варианты “вторжения в разговор”.

[code] BARGE-IN TYPE/ ВИД ВТОРЖЕНИЯ В РАЗГОВОР

(В данном коде назначается вид вторжения в разговор)

[*] NO BARGE-IN Вторжение в разговор запрещено (независимо от класса обслуживания аппарата).

[**] WITH TONE Вторжение в разговор сопровождается предупреждающим сигналом и сообщением на дисплее.

[***] WITHOUT TONE Вторжение в разговор не сопровождается предупреждающим сигналом и сообщением на дисплее системного телефона. Микрофон системного телефона, вторгающегося в разговор, выключен.

Примечание: процедура включения функции “вторжение в разговор” может несколько отличаться для каждой конкретной модели мини-АТС и указывается в соответствующем разделе “Руководства пользователя” на данную мини-АТС.

Прослушивание телефонных переговоров, осуществляемое за счёт функции “Автоматическая запись в систему голосовой почты”.

Данная процедура предназначена для разрешения аппаратам системы (мини-АТС) вести автоматическую запись разговоров.
С помощью программирования АТС можно выбрать запись входящих, исходящих или всех разговоров нужного абонентского аппарата.

[code] AUTO RECORD/ АВТОМАТИЧЕСКАЯ ЗАПИСЬ РАЗГОВОРА
(В данном коде назначается вид автоматической записи)

[*] EXT AREC NO Автоматическая запись внутренних разговоров во внешнюю систему голосовой почты.
[**] VM AREC NO Автоматическая запись разговоров во встроенную систему голосовой почты.
[***] VM REC NO Запись разговоров во встроенную систему голосовой почты.
[****] VMS REC NO Запись разговоров во внешнюю систему голосовой почты.

Примечание: процедура включения функции “автоматическая запись в систему голосовой почты” может несколько отличаться для каждой конкретной модели мини-АТС и указывается в соответствующем разделе “Руководства пользователя” на данную мини-АТС.

Удалённый контроль голосовых сообщений за счёт “дополнительных” функций абонентских устройств телефонной связи.

- В настоящее время некоторые уже стали вообще забывать, что есть такая вещь, как стационарные телефоны. А они еще есть, и достаточно активно используются, и могут иметь функцию “**автоответчик**”.
- И есть ещё абоненты, которые реально пользуются автоответчиком, оставляя на нём голосовые сообщения.
- Многие абонентские устройства сети телефонной связи: телефонные аппараты, “чистые” автоответчики, факсимильные аппараты с автоответчиком, беспроводные телефоны (*в частности, стандарта DECT*) и т.д. имеют ряд штатных **“дополнительных”** функций, позволяющих дистанционно управлять автоответчиком – т.е. фактически контролировать его удалённо.
- Данные функции реализованы в большинстве моделей указанных выше устройств и, в ряде случаев, могут представлять реальную угрозу с точки зрения утечки информации, записанной на автоответчик.
- Необходимо отметить, что данные функции являются **именно “штатными”** – они чётко прописаны в “Инструкции по эксплуатации” этих устройств и, при определённом стечении обстоятельств, ими может воспользоваться грамотный злоумышленник, который умеет “**смотреть на вопросы ширше**”.

Примеры абонентских устройств, имеющих функцию “автоответчик”.

Управление автоответчиком с удаленного телефона

Следующие операции возможны при использовании удаленного кнопочного тонального телефона. Перед уходом включите аппарат на ANS/FAX в режиме AUTO RECEIVE (см. с. 15).

Кнопка набора номера	Команда удаленного управления	Стр.	Кнопка набора номера	Команда удаленного управления	Стр.
1	Повторяет сообщение	52	* 4	Удаляет определенное сообщение	52
2	Пропускает сообщение	52			
4	Воспроизведение нового сообщения	51	* 5	Удаляет все сообщения	52
5	Воспроизведение всех сообщений	51	8 1	Включает функцию передачи сообщений при их поступлении	53
6	Прослушивание звуков в помещении	52	8 2	Выключает функцию передачи сообщений при их поступлении	53
7	Перезапись исходящего сообщения	53			
9	Останавливает перезапись исходящего сообщения	53	0	Пропускает исходящее сообщение	53

Удаленное управление автоответчиком

1. Позвоните на свой аппарат.

2. Введите код удаленного управления во время звучания исходящего сообщения автоответчика [ ][ ][ ].

3. Нажмите кнопку команды в течение 4 секунд (см. справа).
   Или
   Подождите 4 секунды. Будут воспроизведены все записанные сообщения.

Кнопка	Команда
0	Пропускает исходящее сообщение
1	Повторяет сообщение
2	Пропускает сообщение
4	Воспроизведение нового сообщения
5	Воспроизведение всех сообщений
6	Прослушивание звуков в помещении
7	Перезапись исходящего сообщения
9	Останов перезаписи исходящего сообщения
* 4	Удаляет определенное сообщение
* 5	Удаляет все сообщения
8 1	Включает функцию передачи сообщений
8 2	Выключает функцию передачи сообщений

Естественные технические каналы утечки информации: электромагнитный и электрический.

В **электромагнитных каналах утечки информации** носителем информации являются побочные электромагнитные излучения (**ПЭМИ**) – нежелательные (*паразитные*) электромагнитные излучения, возникающие при функционировании технических средств обработки информации.
С точки зрения защиты информации опасность представляют информативные ПЭМИ, содержащие в себе признаки обрабатываемой информации.
В частности, эта угроза актуальна для “кнопочных” телефонных аппаратов, в состав которых входит ряд электронных модулей. При этом, могут возникать как высокочастотные ПЭМИ, в которых высокочастотная “несущая” модулирована речевым сигналом, так и низкочастотные ПЭМИ – например, возникающие вследствие “самовозбуждения” усилителей низкой частоты.

Причинами возникновения **электрических каналов утечки информации** являются наводки информативных сигналов – *под которыми понимаются токи и напряжения в токопроводящих элементах*, вызванные побочными электромагнитными излучениями, ёмкостными и индуктивными связями.

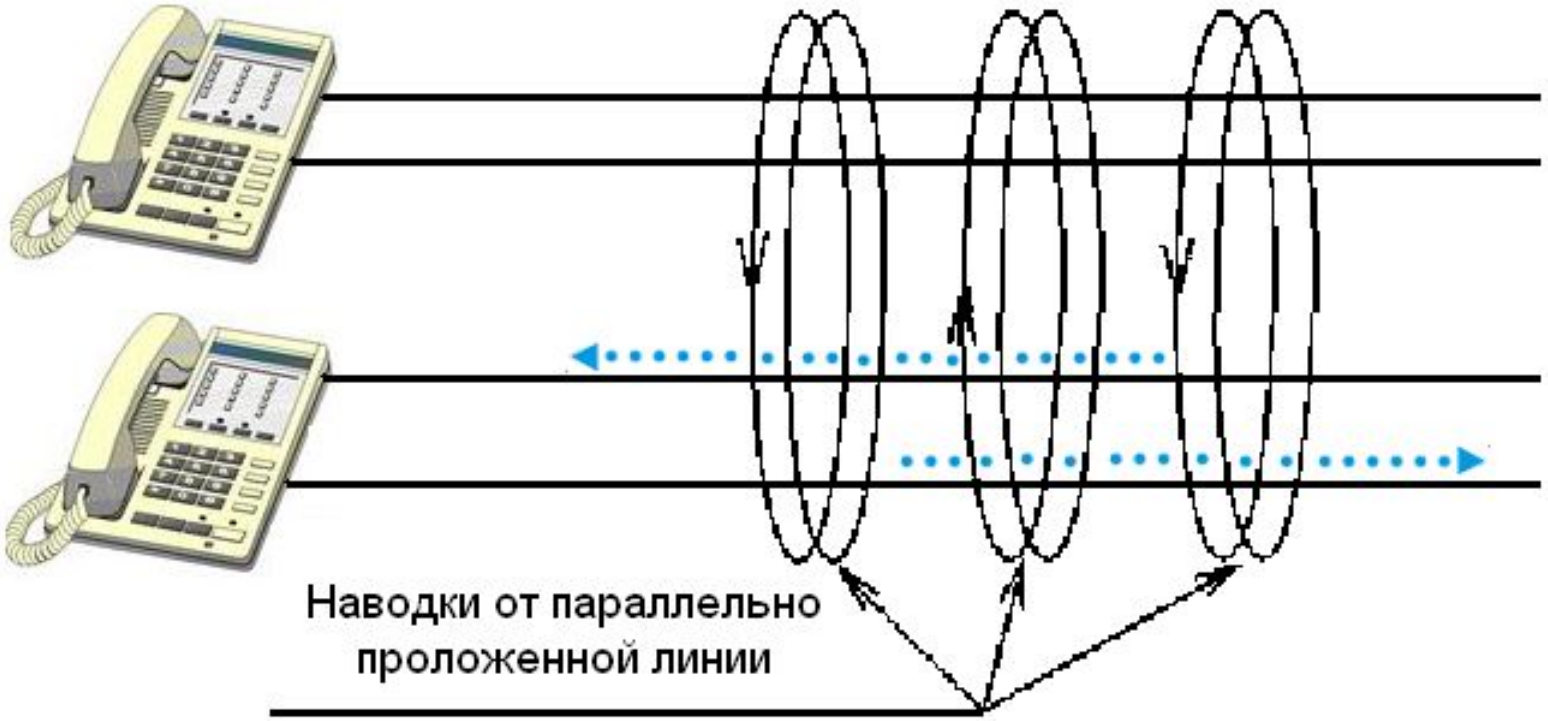
Наверное многие сталкивались с ситуацией, когда во время телефонного разговора слышали в трубке разговор двух других абонентов – обычно “приглушённый” и “далёкий”, но иногда очень чёткий и разборчивый.

Утечка информации, обсуждаемой по телефону, за счёт ПЭМИ.

http://www.pki-electronic.com/products/audio-surveillance-equipment/needle-microphone-with-amplifier-2/

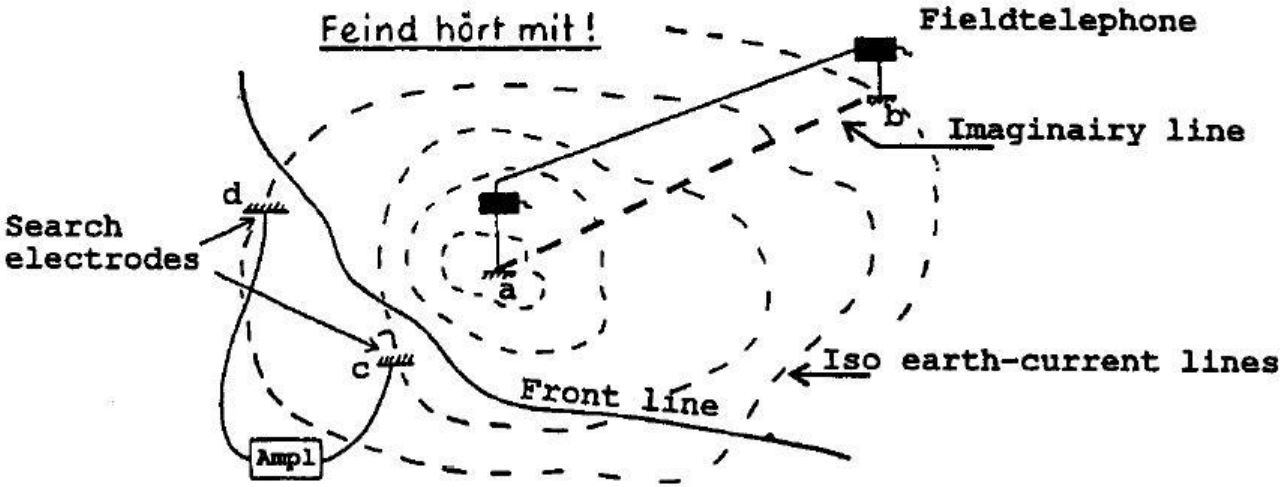
Примеры некоторых ТА, при работе которых могут возникать ПЭМИ.

Наводки информативного сигнала, возникающие при параллельном пробеге телефонных линий.



Примеры из истории.

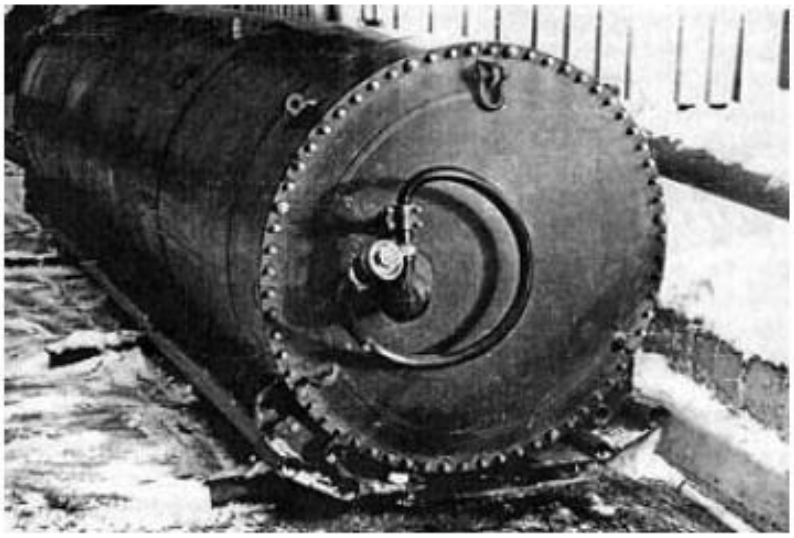
Early use of compromising emanations

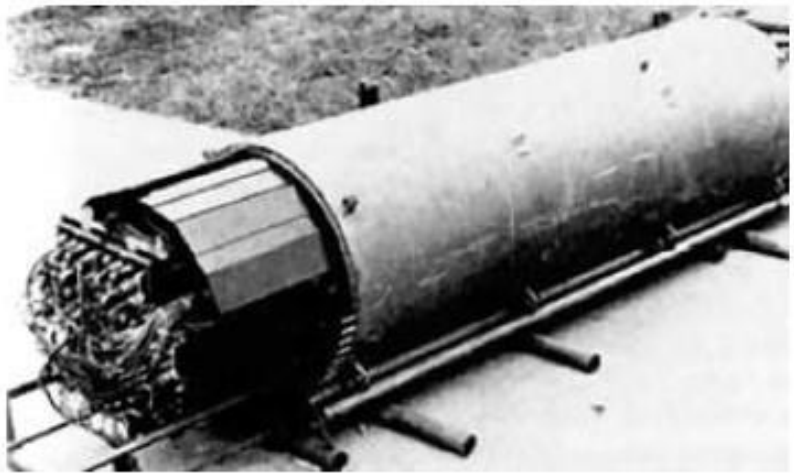


The German army started in 1914 to use valve amplifiers for listening into ground return signals of distant British, French and Russian field telephones across front lines.

Markus G. Kuhn, “Electromagnetic eavesdropping on computers”.

Примеры из истории.





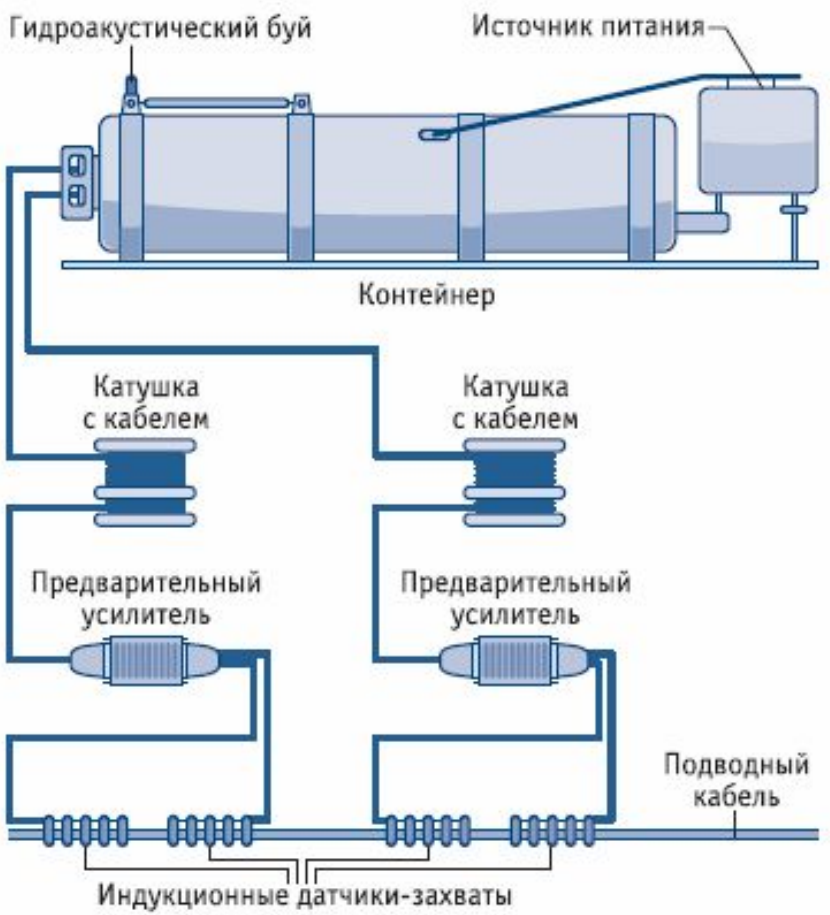
Внешний вид изделия «Камбала»

Индукционный датчик-захват и предварительный усилитель изделия «Камбала»

В 1981 году в Охотском море со дна (глубина 65 м) было поднято подслушивающее устройство, предназначенное для съёма информации с подводного кабеля связи. Поднятое устройство “Камбала” было выполнено в виде стального цилиндра длиной более 5 м, диаметром около 1,2 м и весило порядка 7 тонн. Устройство состояло из двух герметичных контейнеров, в одном из которых размещалась разведывательная аппаратура, а другой представлял собой миниатюрный ядерный (плутониевый) реактор для энергопитания аппаратуры. Расчётный срок работы реактора составлял десятки лет.

Хорев А.А. “Средства перехвата информации с проводных линий связи” / “Защита информации. Инсайд.”, 2011 г. № 1.

Схема перехвата информации с подводной линии связи изделием “Камбала”.



Для “снятия” сигналов с защищённого двойной бронёй из стальной ленты подводного кабеля использовались индукционные датчики-захваты (*магнитные антенны*).
Сигналы с индукционных датчиков предварительно усиливались антенными усилителями, а затем поступали в специальный блок, где было смонтировано электронное оборудование для приёма, усиления, частотного разуплотнения (*демодуляции*) и записи “снятых” с кабеля сигналов.
Запись разговоров осуществлялась автоматически при наличии сигнала в телефонном канале (*режим акустопуска*).
Для записи использовалось 60 магнитофонов, общий объём записи которых превышал три тысячи часов.
Кассеты с записанной информацией из устройства периодически изымались и направлялись для анализа в центр обработки и дешифрования.

Хорев А.А. “Средства перехвата информации с проводных линий связи” / “Защита информации. Инсайд.”, 2011 г. № 1.

Примеры из истории.

Изделие «Крот»

Для перехвата информации с кабельных линий связи, проходящих по суше, в 70-х годах прошлого века американские специалисты разработали устройство “Крот”, использовавшее тот же принцип, что и “Камбала”.

Информация с кабеля “снималась” с помощью специального индукционного датчика. Для его установки использовались кабельные колодцы, через которые проходили телефонные магистральные кабели связи. Датчик в колодце укреплялся на кабеле и для затруднения обнаружения проталкивался в трубу, подводящую кабель к колодцу.
Перехватываемая датчиком информация записывалась на специальный магнитофон. Устройство позволяло осуществлять запись информации, передаваемой одновременно по 60 телефонным каналам.
Продолжительность непрерывной записи разговора на магнитофон составляла около 115 ч.
Устройства серии “Крот” были снабжены радиомаяками, смонтированными в их корпусах. Агент, проезжая или проходя в районе установки устройства, с помощью портативного передатчика пересылал специальный сигнал. Если устройство оставалось никем не тронутым, радиомаяк передавал ответный кодированный сигнал – в этом случае осуществлялась замена диска магнитофона.
Одно из устройств серии “Крот” в 1980-х годах было обнаружено в кабельном колодце недалеко от Московской кольцевой автодороги.

Хорев А.А. “Средства перехвата информации с проводных линий связи” / “Защита информации. Инсайд.”, 2011 г. № 1.

Перехват информации, передаваемой по ВОЛС.

В настоящее время волоконно-оптические линии связи (**ВОЛС**) получают всё большее распространение.

В современных системах связи “оптика” используется не только для соединений между АТС или на магистральном и распределительном участке – часто она “доходит” непосредственно до абонента.

По сравнению с “классическими” кабелями ВОЛС имеют целый ряд преимуществ – *в том числе это касается повышения надёжности и безопасности сетей связи*.

Но при этом нужно чётко понимать, что ВОЛС не являются “панацеей” от всех возможных угроз: при использовании “оптики” минимизируются или полностью устраняются многие “классические” угрозы, но им на смену приходят новые (*иногда основанные на других физических принципах*).

Естественно, что здесь не всё так просто, но в ряде случаев перехват информации, передаваемой по ВОЛС, вполне реален.

Более подробная информация по этому вопросу содержится в учебном курсе “*Информационная безопасность волоконно-оптических технологий*”, автор которого *В.В.Гришачев*.

Варианты перехвата информации, передаваемой по ВОЛС.

ПОДКЛЮЧЕНИЕ К ВОЛОКОННО-ОПТИЧЕСКОМУ КАНАЛУ

сценарии перехвата трафика из волоконно-оптических коммуникаций (1) нарушителем (2):

КОНТАКТНЫЕ МЕТОДЫ:

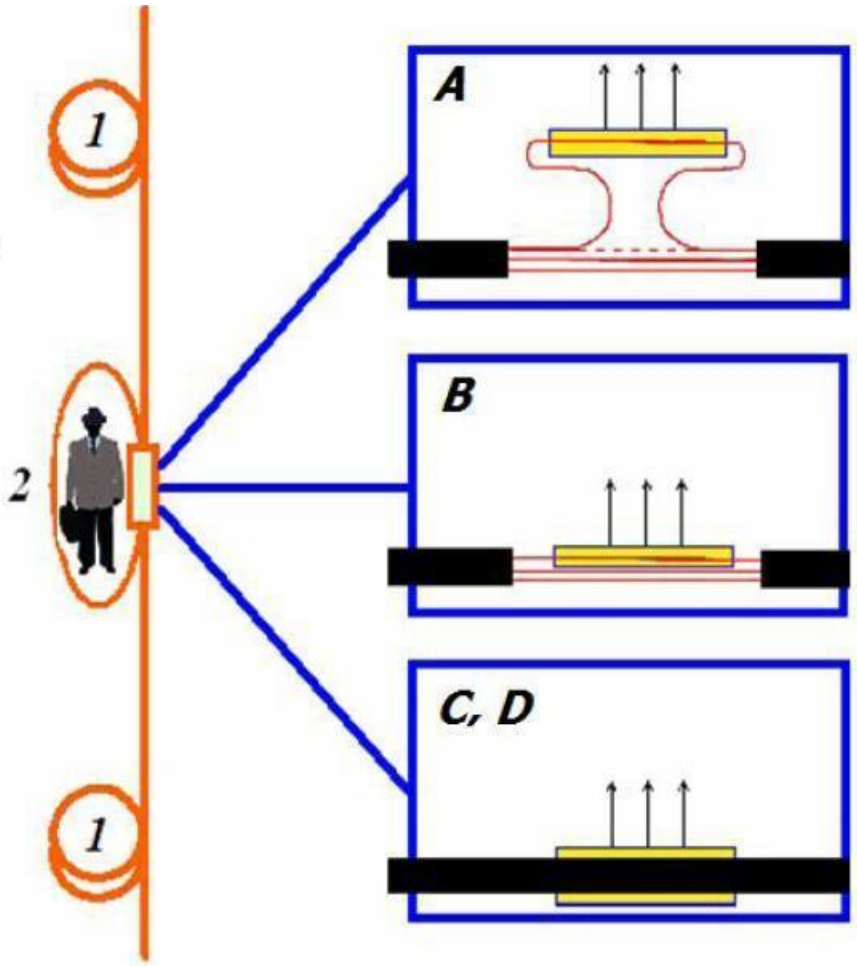
A – контактный перехват с разрывом оптоволокна и вставкой;

B – контактный перехват с прямым доступом к волокну;

ДИСТАНЦИОННЫЕ МЕТОДЫ:

C – дистанционный перехват на основе параметрических методов;

D – дистанционный перехват с регистрацией побочных излучений.



Наиболее вероятные участки контактного подключения к ВОЛС.

ПОДКЛЮЧЕНИЕ К ВОЛОКОННО-ОПТИЧЕСКОМУ КАНАЛУ

Наиболее опасные для перехвата по типу А и В участки структурированной кабельной системы:

1 – защитные оптические муфты для сварных соединений, 2,3 – коммутационно-распределительные устройства (оптические кросс-панели, стойки).

1 2 3

Принцип подключения к ВОЛС с помощью оптоволоконной вставки.

ПОДКЛЮЧЕНИЕ К ВОЛОКОННО-ОПТИЧЕСКОМУ КАНАЛУ

контактный способ с разрывом оптоволокна и подключением оптоволоконной вставки

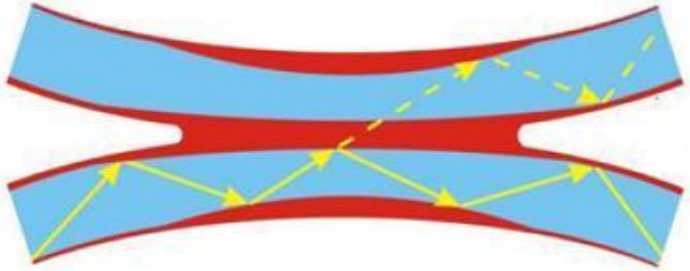
Оптоволоконная вставка – устройство отвода оптического излучения из оптоволокна с минимальными возвратными и прямыми потерями, включаемое в штатную оптическую линию путем его разрыва и замыкания оптического канала через вставку.

Принцип работы сплиттера.

ОТВОД ЧАСТИ ОПТИЧЕСКОГО ИЗЛУЧЕНИЯ

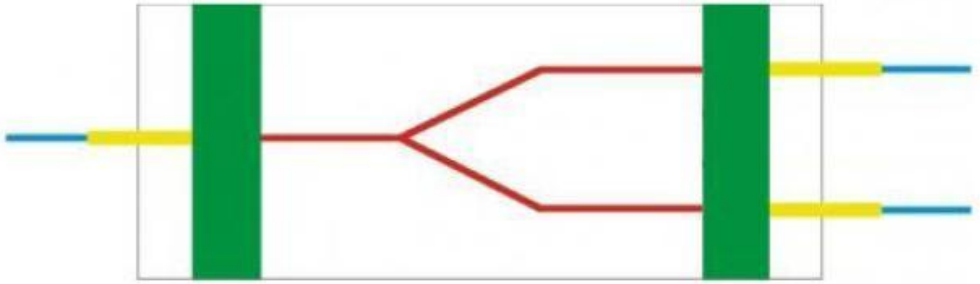
» *Сплиттеры:* выполненные по сплавной технологии Fused Biconic Tapered (FBT)

волокна скручиваются и свариваются



» *Сплиттеры:* выполненные по планарной технологии Planar Lightwave Circuit (PLC)

изготавливаются по
толстопленочной технологии
на кремниевой подложке



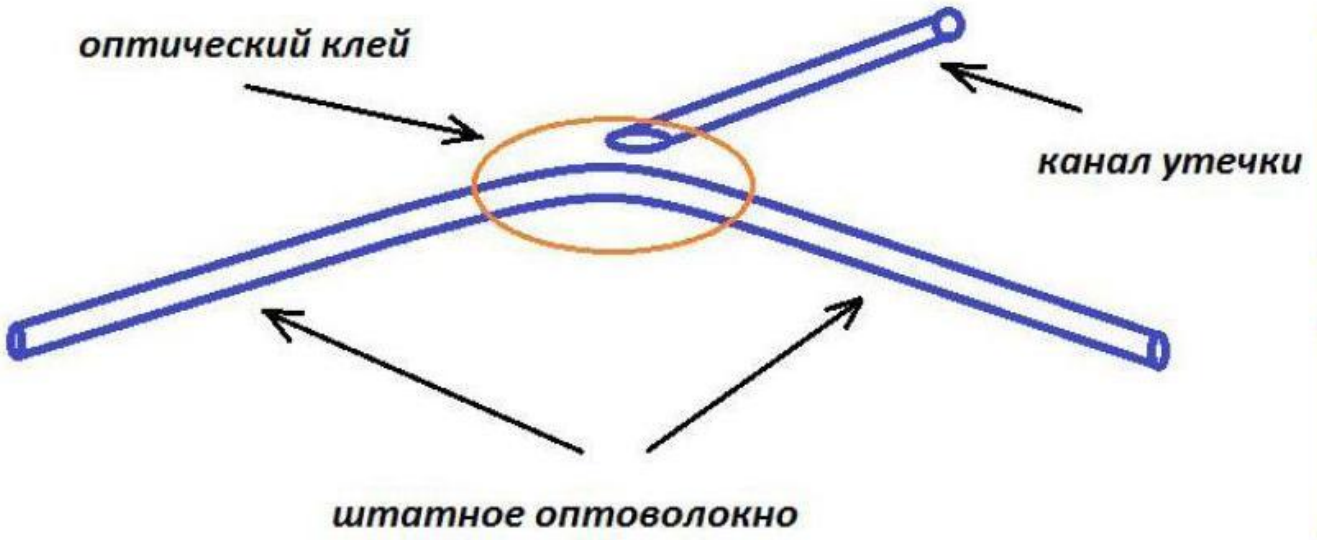
Пример оптического разветвителя (*сплиттера*).

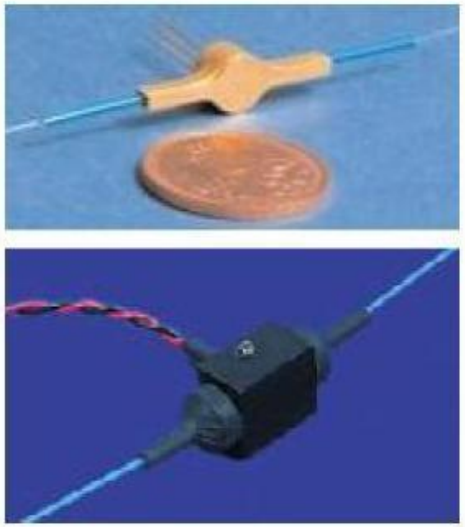
Принцип подключения к ВОЛС за счёт ответвления на макроизгибе.

ПОДКЛЮЧЕНИЕ К ВОЛОКОННО-ОПТИЧЕСКОМУ КАНАЛУ

контактный способ без разрыва оптоволокна – ответвление на макроизгибе

Формирование канала утечки путем отвода оптического излучения из штатного волокна в специальное волокно на макроизгибе (штатные устройства)





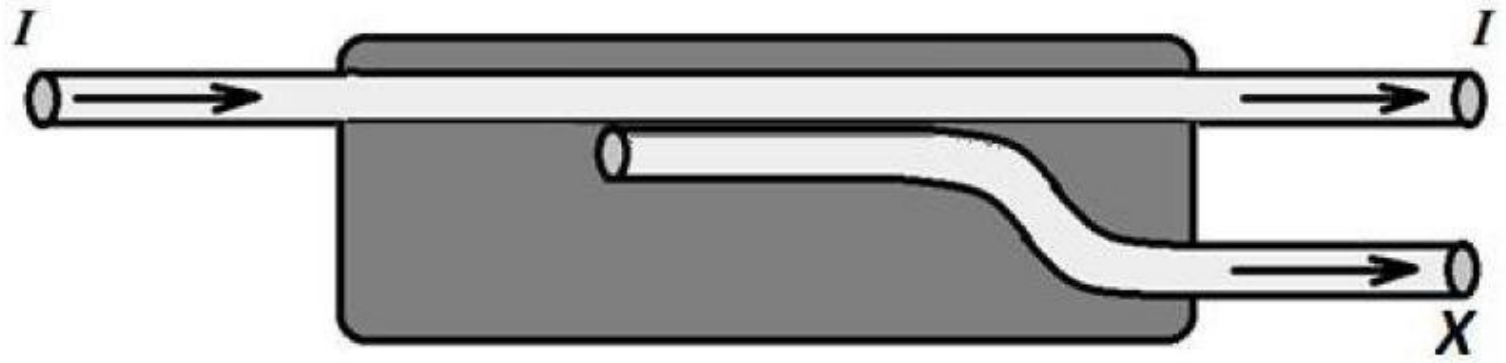
Принцип подключения к ВОЛС за счёт оптического туннелирования.

ПОДКЛЮЧЕНИЕ К ВОЛОКОННО-ОПТИЧЕСКОМУ КАНАЛУ

контактный способ без разрыва оптоволокна –

оптическое туннелирование

интегрально-оптический ответвитель на основе оптического туннелирования



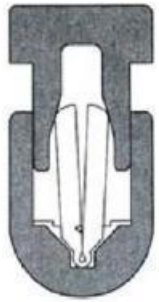
Пример оптического соединителя.

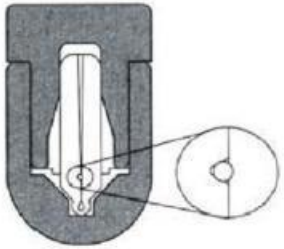
ПОДКЛЮЧЕНИЕ К ВОЛОКОННО-ОПТИЧЕСКОМУ КАНАЛУ

контактный способ без разрыва оптоволокна – оптическое туннелирование

Формирование сигнала утечки путем оптического туннелирования излучения из волокна в специальное волокно, механически сцепленные боковыми поверхностями

Основные элементы Fibrlok™ II 2539



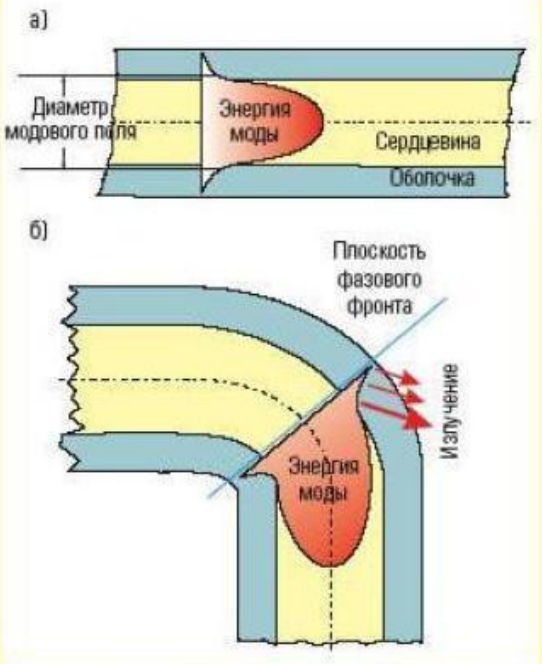


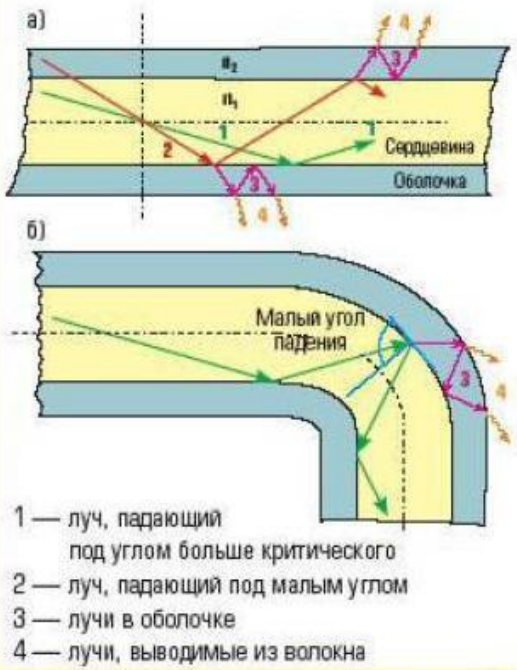
использование для бокового соединения механического соединителя оптических волокон типа FibrLok

Принцип перехвата излучения ВОЛС за счёт его отвода на макроизгибе.

ОТВОД ЧАСТИ ОПТИЧЕСКОГО ИЗЛУЧЕНИЯ

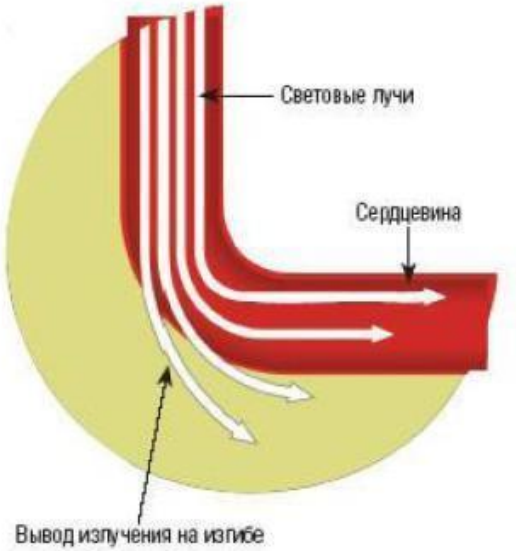
изгиб оптического волокна





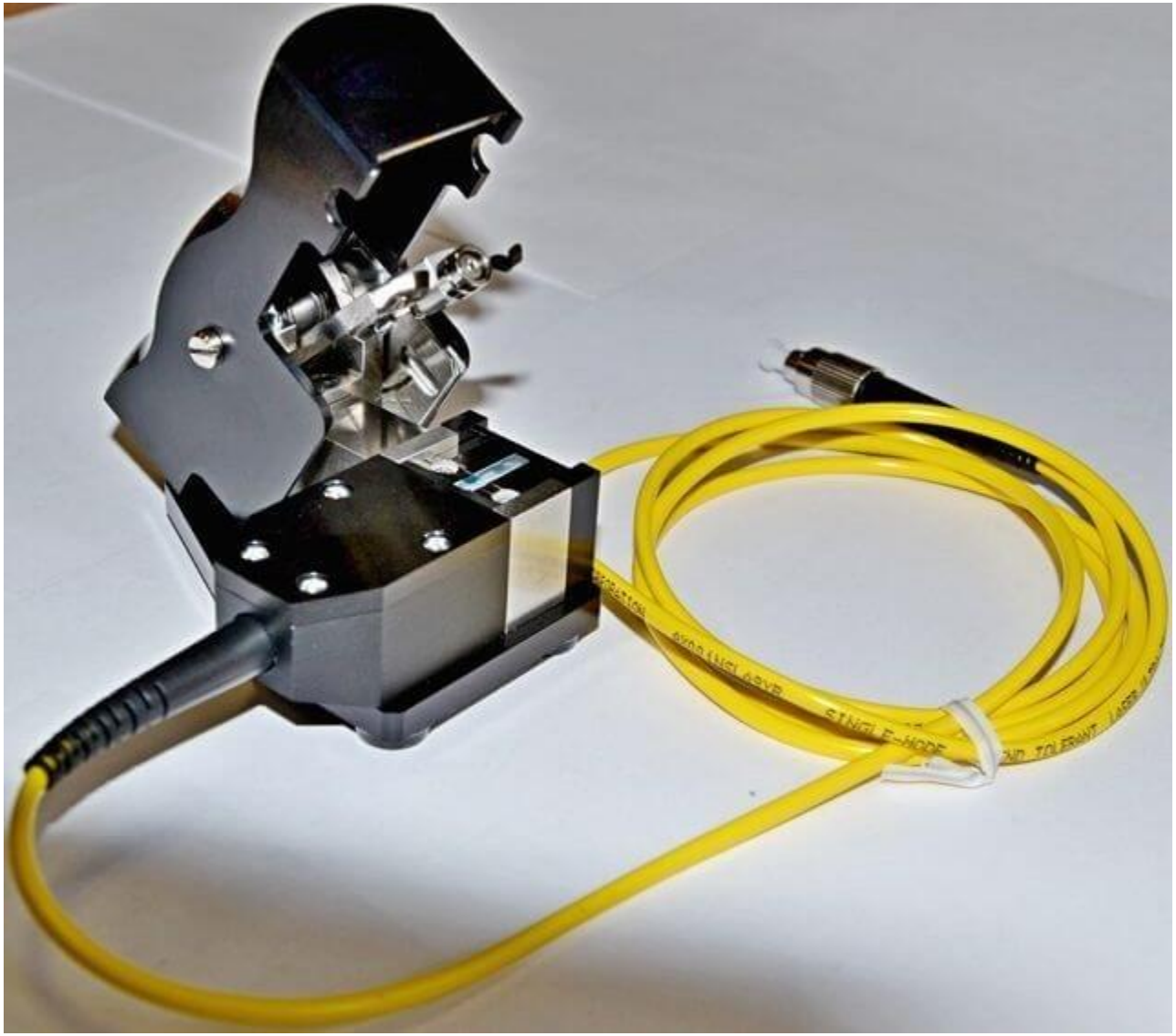
Потери на изгибах, с точки зрения электродинамики:
а — распространение моды в сердцевине волокна;
б — излучение части энергии моды на изгибе

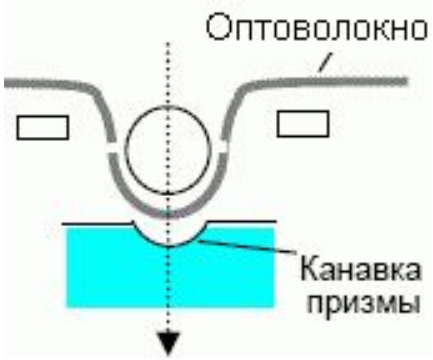
Потери на изгибах с точки зрения геометрической оптики:
а — полное внутренне отражение на прямолинейном участке;
б — части излучения на изгибах из-за нарушения углового условия



отвод излучения на макроизгибе волокна

Пример “ответвителя-прищепки”.





Наиболее вероятные места дистанционного перехвата излучения ВОЛС.

ДИСТАНЦИОННЫЙ СПОСОБ СЪЕМА ИНФОРМАЦИИ

характерные неоднородности оптической структурированной кабельной системы

места соединения и коммутации

оптические кроссы и муфты

места соединения с активным оборудованием, скрутка кабеля

Некоторые факторы, влияющие на уязвимость ВОЛС.

Проведение мероприятий по повышению эффективности перехвата трафика:

- Изменение параметров оптического кабеля внешним воздействием
  - изгиб, скрутка, петля, пережим кабеля
  - воздействие на кабель внешнего физического поля (например, источник радиации вблизи кабеля увеличивает локальные потери, аналогично источник тепла, вода)
  - повреждение оболочки кабеля.
- Использование не декларируемых и не выявленных свойств оптического кабеля
  - не сертифицированный на специальные свойства и воздействия кабель
  - длинные скрученные «хвосты» кабеля
  - другое.

Перехват информации, передаваемой по каналам радиосвязи.

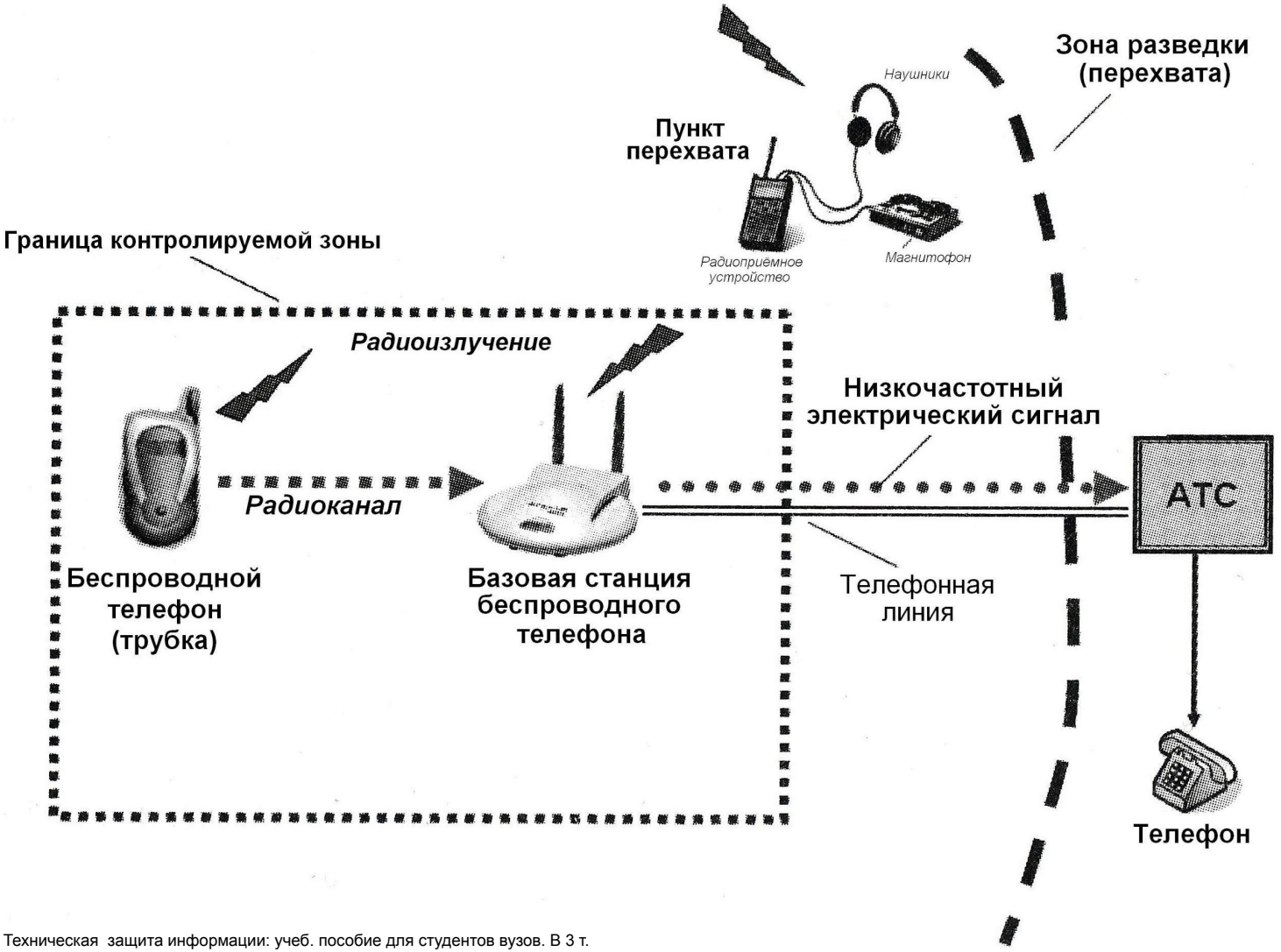
Исходя из “физики работы” – *излучение радиосигнала в окружающее пространство* – системы радиосвязи по определению подвержены возможности перехвата.

Более того, в большинстве случаев факт перехвата информации, передаваемой по каналам радиосвязи, является “безуликовым” и “абсолютно незаметным” – в отличие от “проводных систем”, для подключения к которым злоумышленник должен иметь доступ непосредственно к элементам системы.

Для большинства “обычных” пользователей, ежедневно ведущих разговоры по радиосвязи, наиболее актуальны три вида систем: беспроводной телефон (“*радиоудлинитель*”), транкинговая связь (“*радиостанции*”) и сотовая связь (“*мобильный телефон*”).

Примечание: в связи с массовым наличием “смартфонов” и повсеместным развёртыванием сетей Wi-Fi, актуальным является ведение телефонных и видео разговоров через различные приложения типа Viber, WhatsApp, Telegram и т.п. Вопросы, связанные с перехватом информации в сетях Wi-Fi, в данной презентации не рассматриваются. Угроза, связанная с прослушиванием “мессенджеров”, частично рассматривается в разделе, посвящённом “телефонам-шпионам”.

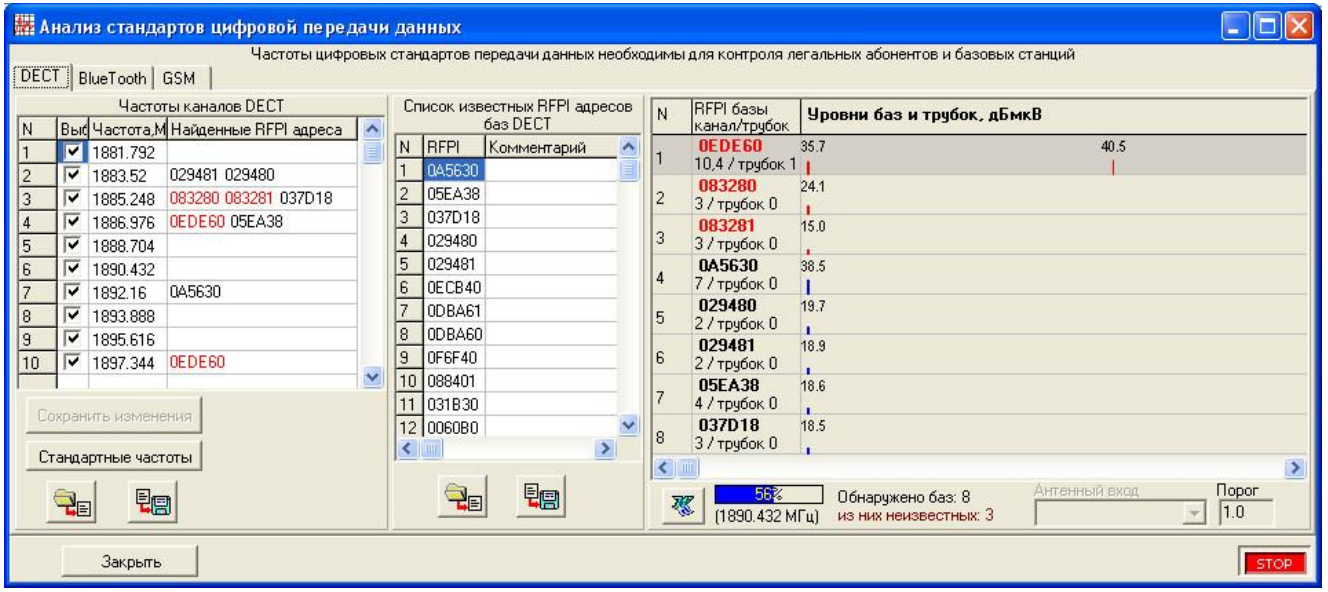
Перехват информации, передаваемой с использованием радиотелефона (“*радиоудлинителя*”).



Хорев А.А. Техническая защита информации: учеб. пособие для студентов вузов. В 3 т. Т. 1. Технические каналы утечки информации. − М.: ООО «НПЦ Аналитика», 2008.

Примеры аналоговых беспроводных телефонов (“*радиоудлинителей*”).

Примеры беспроводных телефонов, работающих в стандарте DECT.



Контроль беспроводных телефонов (“*радиоудлинителей*”).

В зависимости от типа “радиоудлинителя” для его контроля могут использоваться различные технические средства.

В самом простом варианте – *для аналоговых беспроводных телефонов* – достаточно любого связного приёмника соответствующего диапазона.

Для контроля “цифровых” радиотелефонов типа “DECT” потребуется специальный аппаратно-программный комплекс.

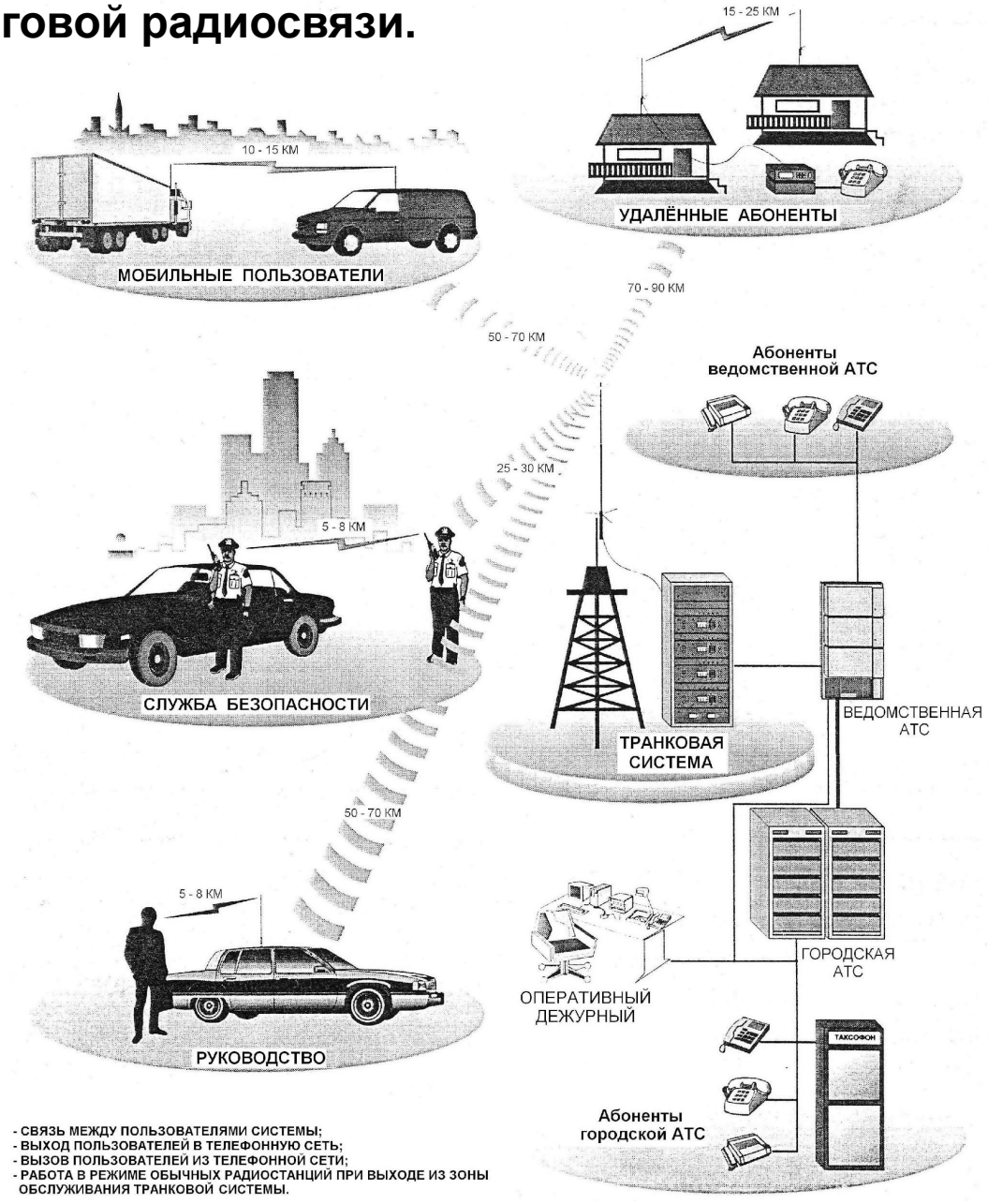
Соответственно, будет отличаться цена оборудования – *от нескольких сотен до нескольких тысяч долларов*

Для контроля аналоговых радиотелефонов возможны различные “самодельные варианты” на базе абонентских трубок соответствующего стандарта.

Для телефонов типа “DECT” возможны варианты с программированием дополнительной трубки – *типа “конференцсвязи”* – если данную функцию поддерживает конкретная модель базовой станции беспроводного телефона.

Системы транкинговой радиосвязи.

Транкинговые системы связи широко используются как коммерческими, так и государственными структурами. В большинстве случаев в коммерческих структурах используют “однозоновую” сеть, которая позволяет осуществлять радиосвязь в радиусе не менее 15 километров (один из основных факторов, определяющих дальность связи – высота размещения базовой антенны). В зависимости от типа системы связи сигнал в эфире может передаваться как в аналоговом, так и в “цифровом” виде, а для защиты переговоров могут применяться различные способы шифрования или “маскирования” передаваемой информации. При этом могут быть различные режимы работы радиостанций: симплекс, полудуплекс или дуплекс.



Контроль систем транкинговой связи.

В зависимости от типа транкинговой системы для её контроля могут быть использованы различные технические средства, цена которых составляет от нескольких сотен до нескольких десятков тысяч долларов.

Для аналоговых систем может быть достаточно связного приёмника соответствующего диапазона частот.

Для контроля “цифровых” систем, как правило, потребуется аппаратно-программный комплекс.

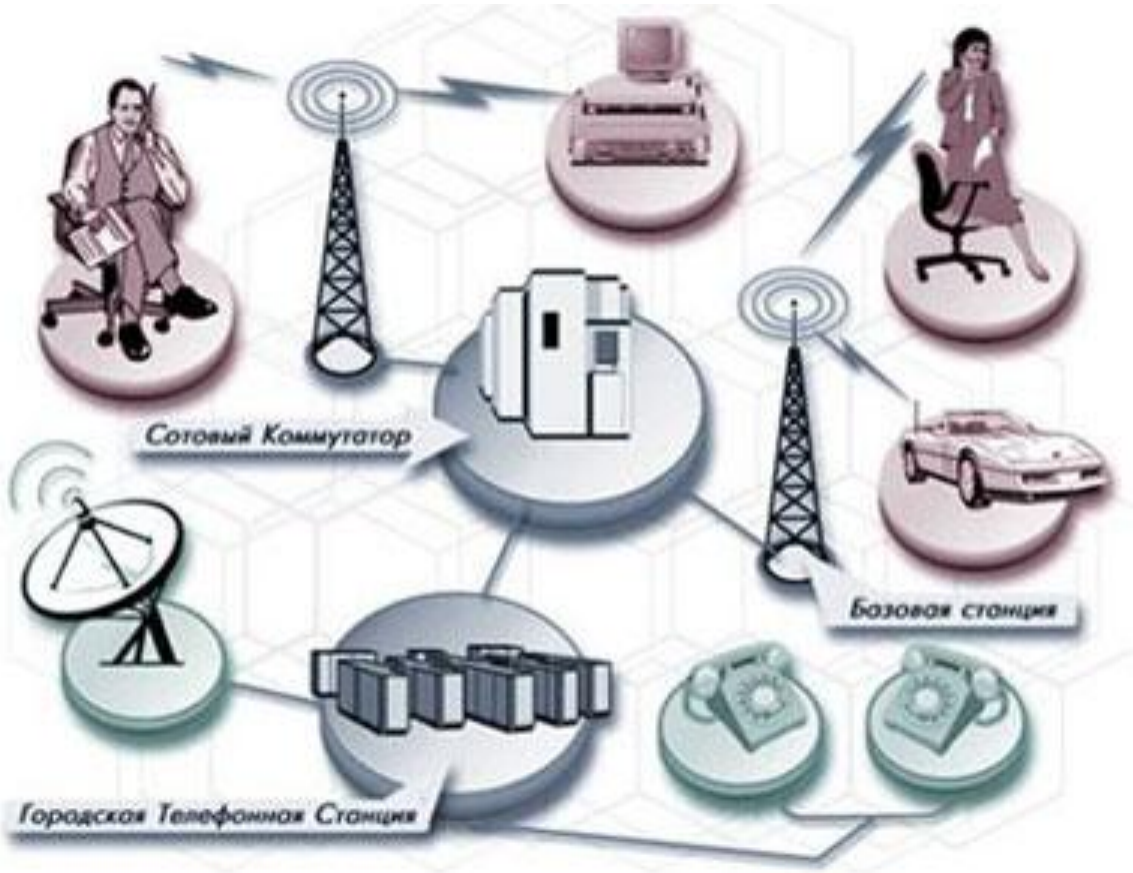
Необходимо заметить, что многие связные приёмники уже имеют возможность демодуляции аналоговых сигналов с инверсией спектра, которая широко применяется для защиты информации в аналоговых системах радиосвязи.

А более дорогие модели (*точнее сказать: “принципиально более дорогие модели”*) имеют возможность декодирования “цифровых” сигналов большинства стандартов – не путать с “дешифрованием зашифрованных переговоров”.

Что касается аппаратно-программных комплексов, то здесь возможности по контролю систем транкинговой радиосвязи ещё выше (*цена, естественно, тоже*) – речь уже идёт не только о декодировании большинства (*практически всех*) известных “цифровых” стандартов транкинговой связи, но и о возможности дешифрования.

Примеры устройств, которые могут использоваться для контроля систем транкинговой связи.

Системы сотовой (мобильной) связи.



Системы сотовой связи в настоящее время очень широко распространены и продолжают развиваться. Учитывая ряд удобств, предоставляемых сотовой связью, некоторые абоненты вообще общаются только с её помощью и практически отказались от услуг фиксированной связи. В то же время, угроза утечки информации, передаваемой с помощью средств сотовой связи, достаточно реальна и это надо чётко понимать.

Перехват информации, передаваемой в сетях сотовой связи.

Условно можно выделить три основных “точки”, в которых может осуществляться перехват информации, передаваемой в сетях сотовой связи:

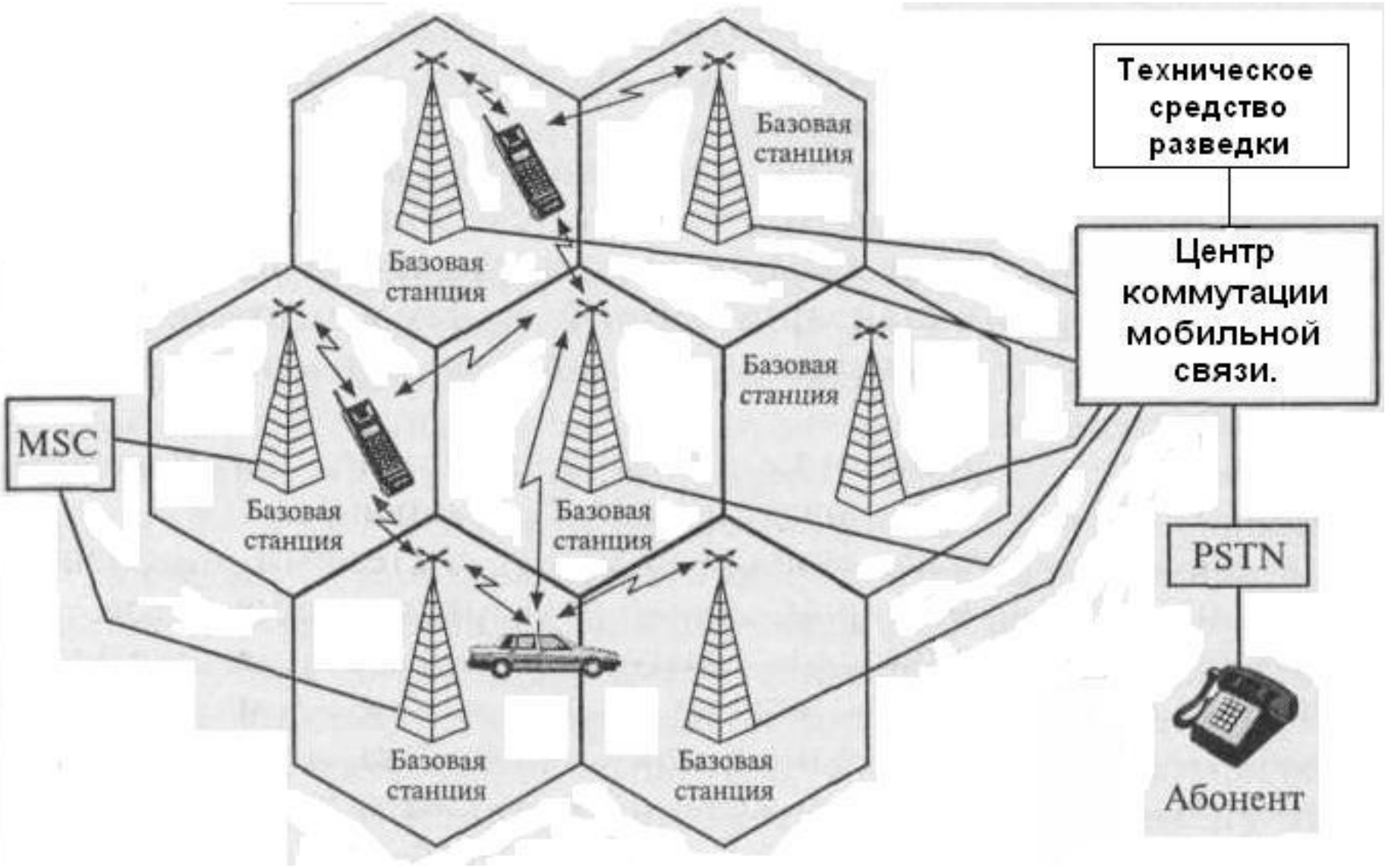
- Съём информации непосредственно в центре коммутации мобильной связи.
- Перехват информации на участке радиоканала “базовая станция – мобильный телефон”.
- Съём информации непосредственно с мобильного телефона за счёт его “модификации” (*так называемый “телефон-шпион”*) или за счёт использования некоторых штатных функций мобильного телефона – *как правило, данные функции доступны в современных моделях мобильных телефонов, в том числе на смартфонах*.

Если рассматривать “коммерческий” вариант перехвата информации, циркулирующей в сетях сотовой связи, то вероятность съёма непосредственно в центре коммутации сети достаточно низка – *речь идёт именно о перехвате телефонного трафика, а не о получении биллинга переговоров*.

Наибольшую опасность в случае “коммерческого” варианта представляет использование “телефонов-шпионов” и перехват информации на участке радиоканала – *при наличии у злоумышленников необходимых технических средств*.

Хочу подчеркнуть: именно “необходимых технических средств” – так как даже при наличии “необходимых финансовых средств” **далеко не каждый сможет достать реально работающий комплекс перехвата**.

Принцип подключения к центру коммутации системы сотовой связи.



Пример стационарного комплекса для мониторинга систем связи.

Digital Telephone Monitoring System

The PKI 1800 is a comprehensive and state-of- the-art end-to-end solution for monitoring, processing, analysis and dissemination of intercepted telecommunication interactions. Due to rapid structural changes in worldwide telecommunication systems a solution integrating all such tasks is provided by the PKI 1800. It offers facilities to monitor ISDN, Digital, PCM30 transmissions as well as all other forms of communication whether they be voice, fax, modem, radio communication or other data transfer. Based on a single, unified platform, PKI 1800 handles all kinds of telephone and Internet data and thus offering unprecedented features. It provides security agencies with flexibility, reliability and versatility in signal intelligence interception and analysis. The PKI 1800 combines all these facilities to comfortably managing unlimited amounts of intercepted communications together with instant target information by just using a minimal amount of space and manpower. The major feature of the PKI 1800 is its flexibility and extraordinary storage capacity, linked to its ability to instantly recall, via the displayed data management target software, intercepted target telephone calls without interrupting the digital tape recording and archiving process. This enables the operator to either carry out interception and playback from one system, or optionally via a separate playback unit. This means that highly classified and priority interception can be configured for transfer by authorised users on a real time basis to a selected location ensuring that the right persons are informed on time.

The PKI 1800 is available in several versions, depending on the number of channels and end-users monitoring requirements, from minimum 8 channels to 64 or max 128 channels. The major criteria of the PKI 1800 software is to display all information immediately and to enable instant evaluation, thus dramatically reducing the time needed, compared to time-consuming evaluation of reel or audio tapes. The software is known as the target evaluation and configuration interface (TEC) which is installed onto the delivered workstation. The sophisticated menu provides optimal guidance for selection/viewing and processing of large quantities of data. The TEC software has one control menu and 4 submenus being linked to user's authorisation key code. They are easiliy accessible and can be seen at a glance on the display monitor. Upon entry to the main control menu selection, the user will see – displayed on the screen – the current channel status which provides activity information as well as remaining tape time, disk end time and selection for the 4 submenus via the preprogrammed password. The configuration menu enables the user to select and change the technical charateristics of each channel depending on the input conditions. This enables the PKI 1800 to monitor telephone interception from various types of exchanges and radio communication input channels simultaneously.

PKI 1800 Digital Playback Unit

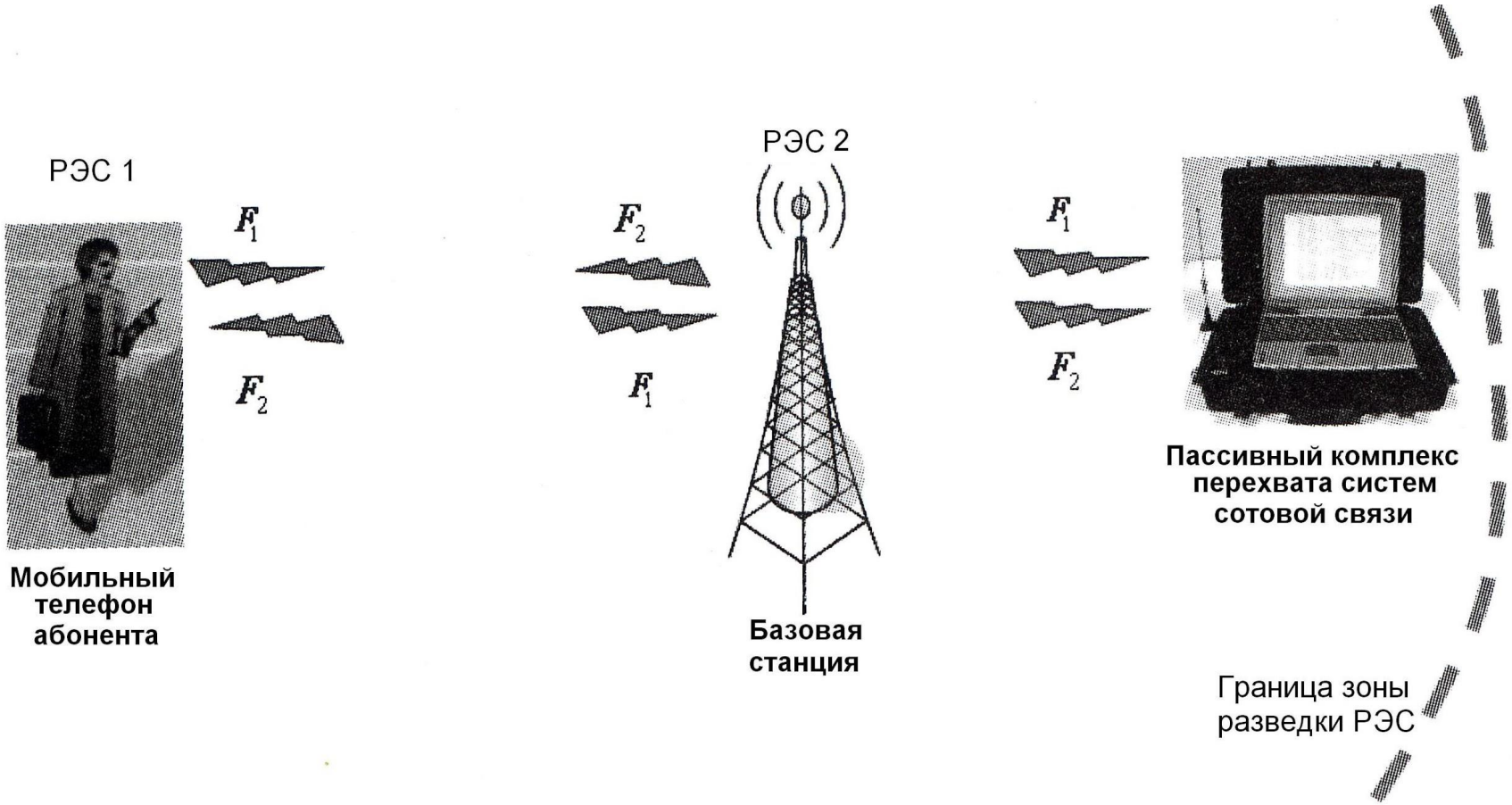
The optional extras available include the digital playback unit which recalls earlier recordings either directly from the DAT cassette of the PKI 1800 or from archived versions. It is an essential accessory to the PKI 1800. Housed in a standard desk top PC with built-in 4 channel voice card, hard disk and loudspeaker the digital playback unit is used for a number of applications. Usually used as a playback unit for evaluation of recorded data it alternatively can be used as a mass storage facility for archiving or as a supervising position. It incorporates the standard PKI 1800 software enabling instant recall and evaluation. The intercepted data is loaded onto the digital playback unit from the DAT cassette or linked to the PKI 1800 for automatic download. The unit can be installed with one or two DAT drives, enabling the evaluated data to be downloaded onto the 2nd drive with the non-essential data being ignored, cancelled or simply kept on the 1st DAT for archiving. The optional extras include a built-in fax and data interception system plus a transcription interface.

Specifications

- Channels: 8, 64 or 128
- Voice interface cards: 4 voice channels per card, each channel digitised to 64 kbits/s using ADPCM conversion. User selectable data compression to 32 kbits/s or 16 kbits/s
- Frequency response: 300 Hz to 3.400 Hz
- Non detectable input impedance
- Simultaneous playback and on-line recording
- Network upgradeable, high MTBF reliability, 1/T1 interception
- Automatic monitoring, interception and recording
- Password protection
- Selectable input characteristics, PABX interfaces
- Analogue/ISDN line, LAN/WAN facility Tape / DVD archiving
- Line inputs: Parallel telephone input impedance – > 30 kOhm (isolated to 3000 V) warning bleep (as CCITT 180)
- Transformer isolated: input impedance – 600 Ohm (isolated to 3000 V)
- E1/T2: 2.048 MHz E1 & 1.544 MHz T2 digital data link
- Line outputs
- Transformer isolated: output impedance
  - 600 Ohm (isolated) output signal – 0 dBm 0=1.23 Vrms
- Monitor output
- Internal speaker
- Headphone jack socket
- Data interface cards: 4 channels per card, synchronous/asynchronous RS232/RS422 serial data data rate up to 64 kbits/s rapid access
- Storage: 1 GB hard disk
- Archival storage: digital audio tape (DAT)
- Recording time: 1 GB hard disk – 1 hr for 64 channels at 32 kbits/s. tape – up to 24 hrs for 64 channels at 32 kbits/s depending on capacity of the storage device
- Reliability: MTBF – 80.000 hours
- Power supply: single phase AC 240/115 V 50/60 Hz
- Power consumption: < 150 W
- Weight:
  - 8 channels 55 kg
  - 128 channels 165 kg
- Dimensions:
  - 8 channels 56 x 38 x 70 cm
  - 128 channels 60 x 157 x 70 cm

http://www.pki-electronic.com/products/interception-and-monitoring-systems/digital-telephone-monitoring-system

Принцип работы пассивного комплекса перехвата систем сотовой связи.



Хорев А.А. Техническая защита информации: учеб. пособие для студентов вузов. В 3 т. Т. 1. Технические каналы утечки информации. − М.: ООО «НПЦ Аналитика», 2008.

Passive GSM Monitoring System for A5.1, A 5.2 (A5.0) Encryption

Specifications

Components:
- Receiver unit, Laptop computer with software, Decyption unit, antenna.
- Frequency ranges: 900/1800 or 850 or 1900 MHz
- Power supply: 12 V DC, 110V – 230V power supply
- Connectors: LAN, antenna, power supply

Receiver unit:
- Dimensions: 320 x 300 x 80 mm
- Weight: 3,8 kg

Decryption unit:
- Dimensions: 320 x 300 x 510 mm
- Weight: 19,8 kg

The PKI 1540 is not limited to A5.2 decryption, but can also decrypt the much more elaborated A5.1 encryption system. The A5.1 encryption is mainly used in Europe and the USA. A localization of the monitoring devices is impossible, as this system works on a passive basis and does not emit any signals. The decryption unit is the main piece of the PKI 1540 in order to decrypt A5.1 encoded conversations. Because such a professional high-capacity processor of course has its price, it is advisable to use only one decryption unit for several monitoring systems. Internet, VPN or LAN can provide the necessary data connections, which, as a further advantage, allows mobile use of this system. This provides a maximum flexibility for numerous monitoring operations.

On request we can also supply a device for stationary use, which also includes the decryption unit. The PKI 1540 is equipped with a receiver unit with a maximum of 32 duplex- channels, a laptop, antenna, power supply and a key decryption unit.

Monitoring of GSM telephone conversations in the near surrounding is possible with both, the handheld device as well as the base station. As all conversations and text messages are recorded on the hard disk of the laptop, an evaluation of the data is possible at any time. PKI 1540 creates a log file listing all telephone numbers of incoming and outgoing calls. The identification of the telephone number of the monitored person can be done with our active systems PKI 1560 or PKI 1580.

With the PKI 1540 it is not possible to find and hold specific mobile phones, because a passive system does not have any influence on the monitored telephones. For this purpose, however, we offer our active systems PKI 1560 and PKI 1580.

The PKI 1540 works in the dual-band range GSM900/1800 or in the single-band range GSM 850 or GSM 1900 and can be equipped with up to 4-32 duplex-channels according to your needs, i.e. it is possible to record a maximum of

32 duplex-channels (both conversation partners). Each receiver unit is equipped with up to 8 duplex-channels.

Пример пассивного комплекса перехвата системы GSM.

http://www.pki-electronic.com/products/interception-and-monitoring-systems/passive-gsm-monitoring-system-for-a5-1-a-5-2-a5-0-encryption/

Пример пассивного комплекса перехвата системы GSM.

Passive GSM Monitoring System for A5.2 (A5.0) Encryption

Specifications

Components:

- Receiver unit, Laptop computer with software, antenna.
- Frequency ranges: 900/1800 or 850 or 1900 MHz
- Power supply: inside 12 V DC, 110V – 230V power supply

Receiver Unit

- Dimensions: 320 x 300 x 80 mm
- Weight: 3,8 kg

The PKI 1520 is a combination of a laptop, the reception unit (the size depends on the desired channels) and the key decryption unit. Power supply and antenna are included in the package.

This system is expandable until up to 32 duplex-channels. Each reception unit disposes of 8 duplex-channels. Recording of all incoming conversations, as well as all text messages is possible.

The controller software allows data evaluation from the laptop's hard disk at any time.

A localization of this passive system is impossible, because it does not emit any active signals. The surveillance of GSM telephone conversation is possible via handheld device as well as via the base station.

PKI 1520 establishes a log file of all telephone numbers of all incoming and outgoing calls. For the identification of the telephone number of the surveyed person our active systems PKI 1560 and PKI 1580 can be used.

Our PKI 1520 allows direct decryption of A5.2 encrypted conversations on the dual-band networks GSM 900/1800 and the single-band networks GSM 1900 or GSM 850.

The system has been developed for mobile use (4-8 duplex-channels) and can be used at any place where conversations shall be monitored.

A similar device developed for stationary use, for example in a car, can also make sense due to its maximal exploitation of 32 duplex-channels and is also available in our product range. Unlike our PKI 1560 and PKI 1580 the stationary system is not able to identify and hold specifically targeted conversations on mobile phones, because it works on a passive basis and therefore does not have any influence on the monitored mobile phone.

http://www.pki-electronic.com/products/interception-and-monitoring-systems/passive-gsm-monitoring-system-for-a5-encryption/

Пример пассивного комплекса перехвата системы CDMA.

CDMA Monitoring System

The PKI 1600 CDMA Monitoring System works in the CDMA 2000 1x and IS95a and b networks. As it works in a completely passive mode, it cannot be located and does not cause any interference in the mobile telephone networks. This system includes a reception unit with antenna as well as a laptop with the monitoring software. It captures the strongest mobile phone transceiver station in the surrounding area and then starts monitoring the conversations, text messages and all data of the persons captured in the reception area. All captured data is stored on the laptop for further evaluation at any time. It is possible to record conversations that have been selected according to specific criteria or to directly listen into the conversation. This might be important, if no other information about the target is known. If due to unfavorable circumstances only one side of the conversation can be captured, the PKI 1600 however continues to record the communication on the remaining channel. Both, stationary and mobile use is possible as it is equipped with all relevant connections.

Specifications

Components:

- Laptop with Windows operating system and controller software, receiver unit, aerial.
- Connection between receiver unit and laptop: USB 2.0 connector.
- Power supply: 12V – 24V, 110V – 230V power supply

Receiver Unit:

- Dimensions: 320 x 300 x 80 mm
- Weight: 3,8 kg

http://www.pki-electronic.com/products/interception-and-monitoring-systems/cdma-monitoring-system/

Принцип работы активного комплекса перехвата систем сотовой связи.

Хорев А.А. Техническая защита информации: учеб. пособие для студентов вузов. В 3 т. Т. 1. Технические каналы утечки информации. − М.: ООО «НПЦ Аналитика», 2008.

Пример активного комплекса перехвата системы GSM.

Active GSM Monitoring System

Specifications

Components:

- Network Access Station, BTS unit, laptop computer with software, antennas.
- Frequency ranges: 900/1800 or 850 or 1900 MHz
- Operating range: 50 – 1000 m
- Power supply: 12 V DC, 110V – 230V power supply
- Connectors: LAN, antennas, power supply.

Network Access Station

- Dimensions: 320 x 300 x 80 mm
- Weight: 3,8 kg

BTS Unit

- Dimensions: 320 x 300 x 80 mm
- Weight:3,8 kg

The PKI 1560 can monitor all connections with A5.2 or A5.0 encryption. Depending on the system of the monitored GSM-network and the used device, it is also possible to monitor and record conversations with A5.1 encryption. The PKI 1560 allows full control of all incoming and outgoing conversations of the monitored mobile phones.

Unlike the passive systems, this device supplies extensive information about the monitored devices, such as IMEI, IMSI, telephone number, and much more. Furthermore, it features numerous search und filtering options in order to locate the target mobile phone.

In combination with our locating device/direction finder PKI 1680 it is possible to specifically track a target mobile phone, even in populated areas. Our active GSM monitoring system works on a fully transparent basis and is completely undetectable.

The detection of all active mobile phones in the near surrounding is done by the IMSI catcher, which offers numerous manipulation possibilities of the target mobile phone's connections.

Establishing a direct contact (call / text message) with the monitored telephones is possible as well. All incoming conversations and text messages are recorded on the hard disk of the laptop.

The PKI 1560 includes the network access station (dual-band), the BTS unit (radio cell) and the laptop with the controller software. Depending on the application area and network quality one or two single-band BTS units are necessary.

http://www.pki-electronic.com/products/interception-and-monitoring-systems/active-gsm-monitoring-system/

Пример активного комплекса перехвата системы GSM.

Active GSM Monitoring System with IMSI Catcher and Decryption Unit

This system leaves nothing to be desired in the field of cellular monitoring. It offers monitoring of all connections with GSM A5.1, A5.2 or A5.0 encryption. Thus, a complete control of all incoming and outgoing conversations of the monitored mobile phone is possible, as well as the identification of all active mobile phones nearby (IMSI catcher).

All incoming conversations and text messages can be stored on the hard disk of the laptop with the controller software.

The decryption unit can be used independently from the monitoring system. All it needs is a data connection, e.g. internet, VPN or LAN between the PKI 1580 and the decryption unit. One decryption unit can be used by several cellular monitoring systems. This also makes sense when using the mobile version, as due to its weight and dimensions the decryption unit is intended for stationary use only.

The active GSM monitoring system has many advantages compared with the passive system, as it captures a lot of information of the monitored mobile phones, e.g. IMEI, IMSI, their own telephone number, and much more. Its search and filtering features offer numerous

possibilities to track the target mobile phone. Furthermore, it features multiple manipulation possibilities concerning the connections of the target phone.

In spite of its numerous features, the PKI 1560 works in a complete transparent manner and remains absolutely undetectable. Of major importance of course is the tracking and locating of the monitored mobile phones. For this purpose we offer different types of locating devices and direction finders, as for example the PKI 1680 and PKI 1700. With these devices it is possible to locate the target mobile phone up to an accuracy of 2 m, even in populated areas.

Our active GSM Monitoring System PKI 1580 includes the network access station (dual-band), the BTS unit, the laptop with the controller software and decryption unit. According to the network quality and place of operation one or two single-band BTS units are necessary. The system can be upgraded to a maximum of 32 duplex channels. This maximum upgrade is intended for stationary use. The version with 4-8 duplex channels with separate decryption unit has been developed for mobile use.

Specifications

Components:
- Network Access Station, BTS Unit, decryption unit, laptop computer with software, antennas.
- Frequency ranges: 900/1800 or 850 or 1900 MHz
- Operating range: 50 – 1000 m
- Power supply: 12 V DC, 110V – 230V power supply
- Connectors: LAN, antennas, power supply.

Network Access Station
- Dimensions: 320 x 300 x 80 mm
- Weight: 3,8 kg

BTS Unit
- Dimensions: 320 x 300 x 80 mm
- Weight: 3,8 kg

Decryption Unit
- Dimensions: 320 x 300 x 510 mm
- Weight: 19,8 kg

http://www.pki-electronic.com/products/interception-and-monitoring-systems/active-gsm-monitoring-system-with-imsi-catcher-and-decryption-unit

Пример “IMSI кэтчера”.

GSM IMSI Catcher

This handy device creates a list of all active (switched on) mobile telephones in your proximity. All captured data, such as IMSI, IMEI are recorded in the data base and can be evaluated at any time. It offers substantial statistical evaluation possibilities of the recorded data.

The PKI 1620 can easily be combined with our PKI 1680 direction finder, a combination that

allows exact locating of a specifically selected mobile phone. Additionally, with the PKI 1620 you have the possibility to selectively block conversations between specific persons.

The GSM IMSI Catcher PKI 1620 comes in a complete set including the laptop and controller software, the BTS unit, antenna and power supply.

Specifications

Components:

- Main device, Laptop computer, BTS unit, antennas, power supply.
- Frequency ranges: 900/1800 or 850 or 1900 MHz
- Power output: 0,1 W – 8W
- Power supply: battery pack inside 12 VDC/5Ah, 110V – 230V power supply
- Size: 320x280x75mm
- Weight: 3,5 kg

http://www.pki-electronic.com/products/interception-and-monitoring-systems/gsm-imsi-catcher

Пример “3G IMSI кэтчера”.

3G UMTS IMSI Catcher

With the PKI 1640 you can catch all active UMTS mobile phones in your proximity. All captured data, such as IMSI, IMEI, TMSI will be stored in the data base and are available for further evaluation at any time. A huge range of statistical data analysis methods is possible. With our 3G UMTS IMSI Catcher you can redirect single UMTS mobile phones to specific GSM frequencies, in order to monitor the conversation with our active or passive cellular monitoring systems. Furthermore, the PKI 1640 allows suppression of specifically selected conversations of targeted persons.

The PKI 1640 comes with BTS unit, laptop with controller software, antenna and power supply.

Specifications

Components:

- Laptop computer, BTS unit, antennas, power supply.
- Frequency ranges: 900/1800 or 850 or 1900 MHz
- Power output: 0,1 W – 8W
- Power supply: battery pack inside 12 VDC/5Ah, 110V – 230V power supply
- Size: 320 x 280 x 75 mm
- Weight: 3,5 kg

http://www.pki-electronic.com/products/interception-and-monitoring-systems/3g-umts-imsi-catcher

“Телефоны-шпионы” – Spy Phones.

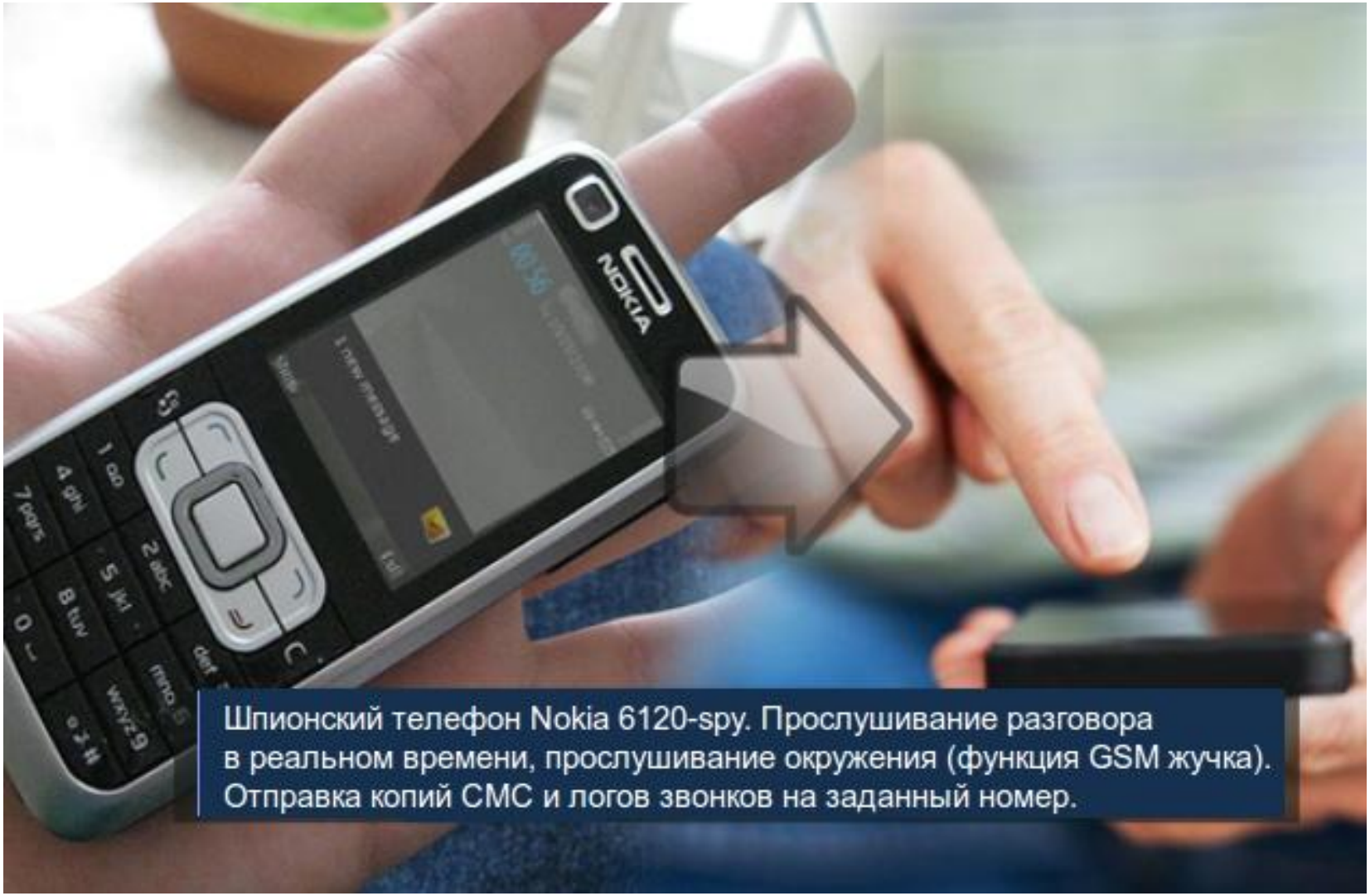
Spy Phone (телефон-шпион) – это устройство, выполненное на базе сотового телефона или смартфона, на который установлено специальное программное обеспечение.

Профессиональный Spy Phone позволяет практически полностью контролировать всю информацию, “проходящую” через данный мобильный телефон: телефонные разговоры, сообщения, данные из памяти телефона, разговоры возле телефона и т.д.

“Телефоны-шпионы” – Spy Phones.

- В последнее время данные устройства активно предлагаются – *в основном через интернет* – и получили достаточно широкое распространение.
- Предлагаемые модели имеют очень большой разброс как по качеству работы, так и по цене. Есть высокотехнологичные профессиональные изделия, есть более-менее хорошие изделия, есть изделия из серии “*третий сорт – не брак*”, есть вообще “левые” и “глюкавые”. Соответственно и цена изделий колеблется в пределах 100 – 2500 долларов.
- По технологии изготовления есть как аппаратно-программные решения (*профессиональные изделия, выполненные на базе любой модели телефона – в том числе на базе “старых” моделей*), так и чисто программные решения, которые могут быть реализованы только на базе современных смартфонов – *причём данные программы совместимы только с конкретными моделями смартфонов*. Кроме того, есть большое количество “самопальных” программ, которые могут устанавливаться “народными умельцами” на смартфоны – это про них (*про программы*): “левые” и “глюкавые”.

Пример “телефона-шпиона”.



Возможности Spy Phone.

Большинство профессиональных “телефонов-шпионов” позволяют:

- дистанционно прослушивать (*записывать*) телефонные разговоры в режиме реального времени;
- вести запись телефонных разговоров на внутреннюю память с последующей передачей их на удалённый компьютер (*телефон*);
- осуществлять отправку копий сообщений на удалённый компьютер (*телефон*);
- прослушивать акустику (*разговоры*) вокруг аппарата – *функция акустической закладки*.

Необходимо понимать, что осуществляется **контроль всех разговоров** и сообщений (*в том числе и передаваемых через WhatsApp, Viber, Telegram и т.п., которые “защищены сквозным шифрованием”*).

В зависимости от технической реализации можно выделить несколько типов “телефонов-шпионов”:

- Spy Phone – Online;
- Spy Phone – Bluetooth;
- Spy Phone – GPRS: в эту условную категорию включены все изделия, которые передают информацию в виде “файла” по каналу передачи данных – *не зависимо от конкретного “протокола” (GPRS, 3G, 4G)*;
- Spy Phone – Dictophone;
- Spy Phone, в котором имеется вторая (“секретная”) SIM-карта, о которой пользователь телефона не подозревает.

Spy Phone – Online

Данное изделие позволяет контролировать телефонные переговоры
в режиме “реального времени”.
При этом, факт “соединения” и “работы на передачу информации”
в ряде случаев будет отражён в детализации у оператора связи,
что является демаскирующим признаком.

Основные функции и режимы работы:

- 1. Контроль акустики - *функция акустической закладки*.
- 2. Контроль разговора при входящем звонке.
- 3. Контроль разговора при исходящем звонке.
- 4. Контроль входящих SMS.
- 5. Контроль исходящих SMS.
- 6. Считывание записных книжек SIM карты и телефона, списков номеров и т.д.
- 7. Дистанционное программирование.
- 8. Блокировка SMS.
- 9. Определение нового номера при смене абонентом SIM карты.
- 10. Определение примерного месторасположения абонента.
- 11. Возможен контроль как с компьютера, так и с мобильного телефона.
- 12. Контроль акустики после разговора.
- 13. Дистанционное управление аппаратом.
- 14. Режим дозвона.
- 15. Автоматическая запись всей полученной информации на жёсткий диск удалённого компьютера (*контрольного пункта*).

Пример Spy Phone Online.

Firefox | Гаджеты Шпиона - Ка... | Прослушка мобильных... | Прослушка мобильных...

espion.me/products/7018761

Google

Каталог товаров / Прослушка мобильных телефонов, шпионские и анти шпионские телефоны

Шпионский телефон BlackBerry 9300 Spy

1599 грн.

В корзину

Позволит вам не только незаметно отслеживать телефонные разговоры его обладателя, но и прослушивать любые разговоры в зоне действия телефона.

До передачи телефона в руки заданной «цели», в секретную область телефона программируется возможность доступа с определенного телефонного номера (процедура подробно описана в прилагаемой инструкции), о существовании которой не сможет узнать ни кто, включая самого объекта слежения. Далее телефон будет работать в соответствии с возможностями, заложенными производителем, а о «дополнительных функциях» своего телефона пользователь никак не узнает. При каждом доступе с запрограммированного номера телефона будет выполнятся один из следующих способов слежения.

НЕОГРАНИЧЕННОЕ ОТСЛЕЖИВНИЕ ПОМЕЩЕНИЯ

Если на неиспользуемый в данный момент телефон позвонить со специального номера, то он автоматически ответит без какой-либо индикации (дисплей, сигнал звонка, подсветка). После того, как телефон ответил на звонок, Вы можете прослушивать все разговоры в радиусе действия шпионского телефона с высоким качеством звука. Если пользователю будет необходимо позвонить, или поступит входящий звонок, то телефон вернется в обычный режим. После окончания разговора пользователем, для продолжения прослушивания помещения, Вам будет необходимо снова позвонить.

НЕОГРАНИЧЕННОЕ ОТСЛЕЖИВНИЕ ТЕЛЕФОНА

Если позвонить на шпионский телефон во время телефонного разговора, независимо от того входящий звонок или исходящий, Вам представится возможность прослушивать разговор обоих собеседников. По окончании разговора Вы сможете перезвонить и вернутся к прослушиванию помещения.

Вы можете позвонить на шпионский телефон из любой части мира, где работает сеть GSM. При попытке исследования телефона на предмет прослушивания, в нем не будет найдено никакой информации о прослушивании, в том числе записи звонков с специального номера. Так же шпионский телефон может отсылать на заданный номер копии всех входящих и исходящих СМС и ММС, логи (номер и время) входящих и исходящих звонков. Доставка почтой и транспортными компаниями. Срок доставки 2-3 дня, по предоплате.

Пример профессионального Spy Phone.

GSM Spy Phone

This is no doubt the most complete solution for the GSM sector. Whether voice or SMS, any communication done with this mobile phone can be monitored by you. As soon as a onversation or an SMS is sent or received with this mobile phone, you receive an information or a copy of the SMS. It can also be used as a bug. A call absolutely unnoticed by the user allows eavesdropping in the vicinity of the mobile phone.

Specifications

- SMS monitoring: Any SMS (sent or received) is copied and transmitted to the number specified by you including date and time, etc.
- Call monitoring: Any call (incoming and outgoing) generates an SM including all necessary data (number, time, etc.). And there is also the possibility to switch in on the conversation unnoticed.
- Room monitoring: A special call allows to monitor conversations held in the vicinity of the mobile phone. This call is absolutely inconspicuous and will not be noticed by the mobile phone user.
- Standard telephone from the current product line equipped with special software for the monitoring functions. Programming of the parameters can be easily done via a PC.

http://www.pki-electronic.com/products/audio-surveillance-equipment/gsm-spy-phone/

Spy Phone – Bluetooth.

ощью Spy Phone – Bluetooth можно сохранять
ормацию – *телефонные разговоры*
ередаваемые сообщения и т.д. –
нутренней памяти телефона, чтобы потом
дать её на компьютер или другой телефон.
роля разговоров нет необходимости всё время
оне действия Bluetooth, так как вся информация
шется во внутреннюю память телефона и
жет быть считана в любое удобное время.

Достоинства перехвата информации относительно режима Online:

- Факт контроля информации не отображается в детализации у оператора – *т.к. работа Bluetooth им не фиксируется*, что обеспечивает безопасность контроля.
- Контроль информации может быть совершенно бесплатным.

Недостатки:

- Небольшое расстояние между контролирующим и контролируемым телефонами для обмена записанной информации – в пределах зоны действия Bluetooth.
- Получение записанной информации с задержкой - не поддерживает контроль телефонных переговоров (*акустики*) в режиме реального времени.

Процедура работы Spy Phone – Bluetooth.

Запись информации:

- Запись всей информации идёт на внутреннюю память контролируемого телефона или на карту памяти. Выбор типа памяти происходит дистанционно и незаметно для пользователя через SMS.
- Файлы с полученной информацией пишутся скрытно и не доступны для просмотра пользователю аппарата. Файлы невозможно увидеть не только на самом телефоне, но и на компьютере – например, через стандартную программу, которая идёт в комплекте с данной моделью телефона.
- В имени записанных файлов указаны номер, направление, дата и время записи разговора, звонка или сообщения.

Активация bluetooth на контролируемом телефоне возможна двумя способами:

- Путем отправки SMS с указанием активировать Bluetooth. SMS принимается аппаратом бесшумно. Bluetooth будет активен, пока его не выключат с помощью другой командной SMS или пока пользователь сам не решит воспользоваться Bluetooth.
- Можно запрограммировать контролируемый телефон через SMS на такой режим, когда телефон будет незаметно активировать Bluetooth с заданной периодичностью на заданный интервал времени.

Процедура получения файлов:

- Подойти к контролируемому телефону на расстояние, при котором возможна работа Bluetooth, в контролирующем телефоне в списке доступных устройств выбрать контролируемый телефон и ввести пароль, который задается при изготовлении телефона. После этого открывается доступ к папкам на контролируемом телефоне (в том числе и к секретным файлам о разговорах и SMS).
- После перекачки секретные файлы автоматически стираются. Вся процедура установления связи контролируемого телефона с “управляющим” телефоном по Bluetooth происходит незаметно, например, пользователь контролируемого телефона может в это время что-то нажимать, заходить в записную книжку, совершать или принимать звонки. Работа Bluetooth полностью параллельна действиям пользователя.
- Управление функциями Spy Phone происходит дистанционно через SMS.

Spy Phone – GPRS.

С помощью **Spy Phone – GPRS** можно сохранять телефонные разговоры абонента, сообщения и “акустику помещения” во внутренней памяти телефона, после чего контролируемый телефон может автоматически отправить эту информацию на электронную почту или на удалённый сервер, где данная информация будет храниться и откуда её можно скачать/прослушать.

Spy Phone – GPRS не поддерживает контроль в режиме реального времени.

Запись информации:

- Запись всей информации идёт во внутреннюю память “телефона-шпиона”. Файлы с полученной информацией пишутся в скрытую папку.
- Файлы невозможно увидеть не только на самом телефоне, но и на компьютере – например, через стандартную программу, которая идёт в комплекте с данной моделью телефона.
- В имени записанных файлов указаны дата и время разговора.
- Файлы могут записываться как на внутреннюю память самого телефона, так и на внешнюю карту памяти. Пользователь с помощью SMS сам выбирает куда писать информацию.

Отправка файлов на электронную почту происходит в двух режимах: по команде в SMS или автоматически – сразу после разговора.

После передачи, накопленные файлы могут стираться автоматически или по команде в SMS.

Отправка записанных фалов с разговорами происходит по GPRS незаметно, например, пользователь телефона может в это время что-то нажимать, заходить в записную книжку и т.д. Передача файлов по GPRS параллельна действиям пользователя.

Управление функциями происходит дистанционно через SMS.

Стоимость контроля ниже, чем в Spy Phone – Online.

Факт передачи информации отображается в детализации у оператора – это касается устройств, передающих данные именно по GPRS. Для смартфонов, работающих в 4G с опцией “Безлимитный интернет”, где идёт постоянный трафик – это “не так актуально”.

Пример Spy Phone.

Firefox | Гаджеты Шпиона - Каталог товаров | Прослушка мобильных телефонов, шп...

espion.me/products/7018781

Google

Каталог товаров / Прослушка мобильных телефонов, шпионские и анти шпионские телефоны

Шпионский телефон Samsung Galaxy Ace с программой для прослушки ShadowGuard

1899 грн.

В корзину

Телефон со встроенной прослушкой позволяет записывать все разговоры, SMS, копировать данные из телефонной книги и списка вызовов.

Все данные собираются в Вашем аккаунте на сайте программы ShadowGuard. Программа не заметна в телефоне и её нельзя удалить даже полной перезагрузкой телефона.
Программа для прослушки сотового позволяет записывать в любой момент времени через микрофон телефона всё происходящее рядом с абонентом. Таким образом программа может быть использована в качестве жучка. Программа жучок позволяет определять координаты телефона как по GPS, так и по сотовым и WiFi сетям. Телефон поставляется с уже установленной программой. Всё, что Вам нужно - это зарегистрироваться в личном кабинете на сайте программы для прослушки сотового и добавить наблюдаемый телефон. После активации лицензии полный функционал программы и все данные с телефона будут доступны в Вашем личном кабинете. В любой момент времени Вы можете прослушать записанный разговор по телефону, прочитать SMS переписку наблюдаемого абонента. Телефон Samsung Galaxy Ace с жучком - хороший подарок Вашему другу, ребенку, партнеру и Вашей второй половинке. Телефон с программой прослушки комплектуется двумя задними крышками - черной и белой.
Основные функции управления наблюдаемым телефоном доступны также с телефона администратора, который можно зарегистрировать в личном кабинете. Через простой SMS запрос на прослушивамый телефон можно узнать местоположение в виде координат и адреса, список последних вызовов, получить и прочесть SMS, а также многое другое. Доставка почтой и транспортными компаниями. Срок доставки 2-3 дня, по предоплате.

Spy Phone – Dictophone.

Spy Phone – Dictophone реализован на базе конкретных моделей телефонов и предназначен для записи информации во внутреннюю память телефона.

- Spy Phone – Dictophone позволяет скрытно осуществлять запись всего, что слышно через микрофон, не зависимо от действий пользователя.
- Телефон в этом режиме используется как обычный диктофон: если идёт разговор по телефону, то записывается телефонный разговор, если телефон находится в режиме ожидания, то пишется акустика – *всё, что слышно вокруг телефона*.
- Запись осуществляется во внутреннюю память телефона и может продолжаться несколько часов.
- Включение записи происходит нажатием и удержанием клавиши, так же происходит и выключение.
- Если запись была включена, то её нельзя остановить никакими действиями пользователя.
- Записанные файлы не прячутся, но на папку, в которую они записываются, можно установить пароль.
- Съём записанной информации происходит не дистанционно по каналу сотовой связи, а при физическом доступе к телефону: через кабель или Bluetooth.

Spy Phone, имеющий вторую “секретную” SIM-карту.

- Данное устройство представляет собой аппаратно-программный комплекс, выполненный на базе мобильного телефона, который имеет вторую – “дополнительную” – SIM-карту – *не путать с мобильными телефонами, имеющими две “штатные” SIM-карты (так называемые “Duos”)*.
- “Дополнительная” SIM-карта скрытно устанавливается в специальный “секретный” слот, находящийся внутри изделия, о котором пользователь мобильного телефона даже не подозревает.
- Изделие имеет те же функции, что и типовой Spy Phone, но принципиальный момент заключается в том, что управление изделием и передача перехваченной им информации осуществляется по каналу “секретной” SIM-карты, а не по каналу “основного” номера.
- По сравнению с “телефонами-шпионами”, которые рассматривались ранее, данное устройство имеет принципиальный плюс: в детализации “основного” номера, которую может взять у оператора связи пользователь телефона, не будет никаких “следов” о сеансах связи для передачи информации – *не важно, был ли это контроль акустики в режиме реального времени или это была передача по GPRS информации, предварительно записанной в память устройства*.

Пример Spy Phone.

Firefox | Гаджеты Шпиона - Каталог товаров | Прослушка мобильных телефонов, шп...

espion.me/products/7180774

Google

Каталог товаров / Прослушка мобильных телефонов, шпионские и анти шпионские телефоны

Шпионский телефон – прослушка Nokia 6120 spy

1550 грн.

В корзину

Телефон полностью готов к работе. Все что от Вас требуется до передачи телефона в руки заданной «цели», так это вставить секретную сим-карту любого GSM оператора в потайной слот внутри корпуса телефона.

Об этой сим карте объект слежения ни как не догадается. Таким образом, создается возможность скрытого доступа с определенного телефонного номера (процедура подробно описана в прилагаемой инструкции), о существовании которой не сможет узнать ни кто, включая самого объекта слежения. Далее телефон будет работать в соответствии с возможностями, заложенными производителем, а о «дополнительных функциях» своего телефона пользователь не узнает. Для исключения возможности дозвона на номер скрытой сим-карты посторонними лицами, на "шпионской" сим карте сохраняются номера, с которых разрешен доступ. На звонки с других номеров телефон реагировать не будет. При каждом доступе с запрограммированного номера телефона будет выполнятся один из следующих способов слежения.

НЕОГРАНИЧЕННОЕ ОТСЛЕЖИВНИЕ ПОМЕЩЕНИЯ

Если на неиспользуемый в данный момент телефон позвонить со специального номера, то он автоматически ответит без какой-либо индикации (дисплей, сигнал звонка, подсветка). После того, как телефон ответил на звонок, Вы можете прослушивать все разговоры в радиусе действия шпионского телефона с высоким качеством звука. Если пользователю будет необходимо позвонить, или поступит входящий звонок, то телефон вернется в обычный режим. После окончания разговора пользователем, для продолжения прослушивания помещения, Вам будет необходимо снова позвонить.

НЕОГРАНИЧЕННОЕ ОТСЛЕЖИВНИЕ ТЕЛЕФОНА

Если позвонить на шпионский телефон во время телефонного разговора, независимо от того входящий звонок или исходящий, Вам представится возможность прослушивать разговор обоих собеседников. По окончании разговора Вы сможете перезвонить и вернутся к прослушиванию помещения.

Вы можете позвонить на шпионский телефон из любой части мира, где работает сеть GSM. При попытке исследования телефона на предмет прослушивания, в нем не будет найдено никакой информации о прослушивании, в том числе записи звонков с специального номера. Так же шпионский телефон может отсылать на заданный номер копии всех входящих и исходящих СМС и ММС, логи (номер и время) входящих и исходящих звонков. Доставка почтой и транспортными компаниями. Срок доставки 2-3 дня, предоплата обязательна.

Опция “диктофон” в некоторых моделях мобильных телефонов.

Опция “диктофон”, которая позволяет записывать телефонные разговоры в память телефона, есть практически в любом современном мобильном телефоне или смартфоне.
При “штатной работе” мобильного телефона его владелец должен “нажать соответствующую кнопку” (*запустить нужное приложение*).
Однако в некоторых моделях эта функция может включаться автоматически при начале телефонного разговора – *если были заданы соответствующие настройки*.
Трудно сказать, кто и как воспользуется этими записями – *особенно если к телефону имеется доступ посторонних, а владелец телефона не серьёзно относится к этому серьёзному вопросу*.

Заключение.

В заключении несколько слов об основных целях данной презентации:

- Во-первых, наглядно показать перечень возможных угроз – *во всяком случае, как я их вижу* – чтобы у слушателей появилось более-менее ясное представление о том *“что нужно искать” и “от чего нужно защищаться”*.
- Во-вторых, обратить особое внимание на некоторые угрозы, которые представляют наибольшую опасность в реальной жизни – *тут уже каждый решает сам, что он считает наиболее реальным/опасным в своей конкретной ситуации*.
- В-третьих, обратить внимание на то, что ряд современных средств съёма информации (*например, в случае “телефона-шпиона” или при использовании “дополнительных функций” мини-АТС*) требуют принципиально иного подхода к их обнаружению, а что касается радиосвязи (*в случае “пассивного” перехвата*) – вообще не могут быть обнаружены.
- В-четвёртых, попытаться (*по мере возможности*) объяснить “неподготовленным слушателям”, что в реальной жизни “не всё так красиво и романтично” и для поиска возможных каналов утечки информации нужно лазить по кабельным колодцам, подвалам, чердакам, коммуникационным стоякам – везде где проходят кабельные коммуникации, вскрывать кабель-каналы, разбирать абонентские устройства, “сопровождать” работы по ремонту оборудования и т.д.
- В-пятых, напомнить про **здравый смысл и бдительность** – *в хорошем смысле этого слова* **–** что **самое главное**.

Ссылки.

- Хорев А.А. Техническая защита информации. т.1. Технические каналы утечки информации. – М.: ООО “НПЦ Аналитика”, 2008.
- Гришачев В.В. “Информационная безопасность волоконно-оптических технологий”.
- Руководство по эксплуатации на телефонный автоответчик ТЕХЕТ, модель ТХ-235/85.
- Инструкция по эксплуатации на факсимильный аппарат Panasonic KXF680/780.
- Руководство пользователя. Усовершенствованная гибридная система Panasonic KX-TEA308.
- Руководство по функциям. Усовершенствованная гибридная система Panasonic KX-TEA308.

Ссылки.

- www.analitika.info
- www.bnti.ru
- www.ess.ru
- www.gcomtech.com
- www.gedion.lt
- www.integrapro.ru
- www.pki-electronic.com
- www.radioscanner.ru
- www.ray-spyphones.com
- www.reicom.ru
- www.suritel.ru
- www.spyshop-online.com
- www.spycatcher.uk.com
- www.storm-secure.de
- www.telesys.ru
- www.vrtp.ru