ПРАКТИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО ПРИМЕНЕНИЮ СРЕДСТВ И СИСТЕМ СВЯЗИ В УСЛОВИЯХ ПРОВЕДЕНИЯ СПЕЦИАЛЬНОЙ ВОЕННОЙ ОПЕРАЦИИ

Москва 2023

УДК 621.39
П 69

Практические рекомендации по применению средств и систем связи в условиях специальной военной операции.

Практические рекомендации по применению средств и систем связи разработаны для сотрудников силовых структур в условиях Специальной военной операции. Материалы содержат краткие сведения о принципах работы средств подвижной связи, мобильных телефонах, радиообмене, пеленгации. Сведения будут полезны для понимания работы радиотехнических средств с точки зрения защищённого радиообмена в условиях пеленгации и рекомендации по увеличению дальности радиосвязи.

Содержание

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ 4
ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ 6
ПРЕДИСЛОВИЕ 7
1. ОБЩИЕ УКАЗАНИЯ ПО РАДИОЧАСТОТНОМУ ПЛАНИРОВАНИЮ И ОБОРУДОВАНИЮ 8
2. ВЕДЕНИЕ ПЕРЕГОВОРОВ 11
3. ТЕОРИЯ РАДИОСВЯЗИ 12
3.1 Цифровая и аналоговая связь 12
3.2 Системы подвижной связи 13
4. РЕКОМЕНДАЦИИ ПО ИСПОЛЬЗОВАНИЮ СРЕДСТВ И СИСТЕМ РАДИОСВЯЗИ ОВД РОССИЙСКОЙ ФЕДЕРАЦИИ 16
5. УКАЗАНИЯ ПО ИСПОЛЬЗОВАНИЮ МОБИЛЬНЫХ ТЕЛЕФОНОВ 20
5.1 Принцип работы 20
5.2 Мобильный роуминг 21
5.3 Точка доступа (Wi-Fi) 23
5.4 Идентификация личности 23
5.5 Мобильные приложения и другие функции 25
5.6 Рекомендации по ведению сеансов связи с использованием мобильного телефона 27
6. ПЕЛЕНГАЦИЯ РАДИОСРЕДСТВ 29
6.1 Рекомендации по радиообмену в условиях пеленгации 32
7. РЕКОМЕНДАЦИИ ПО УВЕЛИЧЕНИЮ ДАЛЬНОСТИ РАДИОСВЯЗИ ... 36

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

В данных рекомендациях применяются следующие термины и определения:

DMR – открытый стандарт радиосвязи, созданный для пользователей профессиональной мобильной радиосвязи.

MESH-сеть – сетевая топология, построенная на принципе ячеек, в которой рабочие станции сети присоединяются друг с другом и способны принимать на себя роль коммутатора для остальных участников.

Аналоговый сигнал – сигнал представляющий собой непрерывную волну, которая постоянно меняется в течение определенного периода времени.

Клетка Фарадея – устройство экранирования аппаратуры от внешних электромагнитных излучений. Работает по принципу, согласно которому при столкновении электромагнитного поля с чем-то, способным проводить электричество, электрические заряды остаются снаружи проводника, и не могут попасть внутрь.

Конвенциональная система связи – это система связи (может быть аналоговой, цифровой или смешанной), в которой каждая группа абонентов закрепляется за определенной радиочастотой. Когда одна группа занимает один канал связи, остальные вынуждены ждать, пока он освободится.

Радиоэлектронная борьба – разновидность вооруженной борьбы, в ходе которой осуществляется воздействие радиоизлучениями на радиоэлектронные средства систем управления, связи и разведки противника в целях изменения качества циркулирующей в них информации.

Ретранслятор – оборудование связи, которое соединяет два или более радиопередатчика, удаленные друг от друга на большие расстояния. Используется в случаях отсутствия прямой видимости между абонентами или при их расположении относительно друг друга, значительно превышающим возможности действия радиостанции.

Роуминг – процедура предоставления услуг связи абоненту вне зоны обслуживания "домашней сети", за счёт использования ресурсов другой сети.

Система подвижной связи – совокупность технических средств (радиооборудование, коммуникационное оборудование, соединительные линии) с помощью которых можно предоставить подвижным абонентам связь между собой.

Транкинговая система связи – это система связи, в которой происходит автоматическое распределение свободных каналов связи между абонентами через базовую станцию.

Цифровой сигнал – сигнал в виде непрерывной волны, которая несет информацию в двоичном формате и имеет дискретные (конечные) значения.

Чип памяти – микрочип, используемый в качестве хранилища для компьютеров и других устройств.

ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

В данных рекомендациях применяются следующие обозначения и сокращения:

DMR	−	Digital Mobile Radio (Цифровое мобильное радио)
БС	−	Базовая станция
КЗИ	−	Криптографическая защита информации
КСС	−	Конвенциональная система связи
ПРД	−	Передатчик
ПРМ	−	Приёмник
РЭБ	−	Радиоэлектронная борьба
СВО	−	Специальная военная операция
СПС	−	Системы подвижной связи
ТСС	−	Транкинговая система связи

ПРЕДИСЛОВИЕ

Данные рекомендации разработаны для сотрудников силовых структур, выполняющих задачи, в условиях Специальной военной операции (СВО). Материалы содержат краткие сведения о принципах работы средств подвижной связи, мобильных телефонах, радиообмене, пеленгации. Приведённая далее информация, будет полезна для понимания работы радиотехнических средств с точки зрения защищённого радиообмена в условиях пеленгации и рекомендации по увеличению дальности радиосвязи.

Главный принцип, обобщающий все советы и рекомендации по ведению радиосвязи, звучит так: **«Меньше говоришь – дольше проживёшь»**. В широком смысле здесь подразумевается, что абсолютно безопасного способа связи не существует. Поэтому всегда необходимо считать, что связь прослушивается и пеленгуется. Важно хорошо изучить не только боевую и специальную технику, но и методы и средства связи; правильно и умело использовать средства связи в зависимости от складывающейся обстановки; уметь применять технические средства, осложняющие обнаружение сканерами и увеличивающие дальность радиосвязи в условиях действия помех.

Не стоит недооценивать важность подготовки к работе в условиях проведения СВО. Помните про девиз: «Победа любит подготовленных». Предварительно изучите инструкцию (руководство) по эксплуатации на то радиосредство, которое планируете использовать. Особое внимание уделите вопросам безопасности использования, методам скрытого радиообмена, маскирования/кодирования/шифрования информации. При этом помните, что если это не средства криптографической защиты информации, то они защищают только от прослушивания обычным сканером.

1. ОБЩИЕ УКАЗАНИЯ ПО РАДИОЧАСТОТНОМУ ПЛАНИРОВАНИЮ И ОБОРУДОВАНИЮ

Для обеспечения радиосвязи должны быть предусмотрены следующие радиоданные: рабочие радиочастоты, позывные, радиопароли, ключи маскирования/кодирования (если предусмотрены радиостанцией).

Режим работы, рабочие частоты определяются сотрудниками, организующими радиосвязь. При выборе радиочастот необходимо учитывать расположенные в непосредственной близости подразделения. Организовать связь необходимо таким образом, чтобы рабочие радиочастоты Вашего и соседних подразделений не совпадали. Тогда, Вы не будете мешать друг другу.

Если есть потребность в связи с соседними подразделениями, то организуйте отдельный канал связи и для бесперебойной связи – резервные радиочастоты.

Примерная дальность радиостанций УКВ-диапазона (140-470 МГц):

носимые: от 1 до 15 км;

автомобильные: от 3 до 30 км;

базовые: до 45 км.

Дальность радиосвязи зависит от рельефа местности (в том числе перепадов высот), плотности застройки, высоты подвеса антенны и т. д. Более подробные рекомендации даны в разделе 7 «Рекомендации по увеличению дальности радиосвязи».

Для каждой радиосети (радионаправления) в выделенном частотном диапазоне назначаются основной и резервный радиоканалы. Радиосвязь может подавляться противником, поэтому обязательно должны быть предусмотрены резервные радиоканалы, которые программируются («прошиваются») в радиостанции сотрудником, отвечающим за связь. Такими частотами разрешается пользоваться только в случае, если радиообмен по основной частоте невозможен. Решение о переходе на резервные радиочастоты принимается командиром подразделения.

На каждую радиостанцию назначают микрофонные позывные, т. е. псевдонимы, необходимые для того, чтобы не раскрывать личность сотрудника

и сделать невозможным поиск по его реальному имени. Микрофонные позывные применяются при работе с голосовыми вызовами в соответствии с правилами радиообмена. Более подробно об использовании позывных написано в разделе 2 «Рекомендации по ведению переговоров».

При организации радиосвязи внимательно изучите инструкцию по эксплуатации и технические характеристики используемого оборудования. Обратите особое внимание на методы шифрования/маскирования/кодирования радиосигналов в канале. Выясните, как эффективно эксплуатировать эти функции при работе радиостанции.

ВАЖНО! Помните, что если это не средства криптографической защиты информации (КЗИ), то они защищают только от прослушивания обычным сканером.

Во избежание помех от электромагнитного излучения старайтесь не располагать приемопередающее оборудование связи рядом с источниками высоких электромагнитных полей (например, радиолокационными станциями, средствами радиоэлектронной борьбы (РЭБ), станциями спутниковой связи), вблизи электрических проводов высокого напряжения, а также металлических конструкций.

По возможности избегайте создания больших радиосетей (радиогрупп), когда на одной частоте (канале) работают более 30 корреспондентов, с которыми и предполагается активный двусторонний радиообмен. Корреспондентов, работающих в режиме ожидания команды, т. е. приёма, может быть на порядок больше.

Перед эксплуатацией радиооборудования проинструктируйте личный состав об особенностях (как положительных, так и отрицательных) используемых средств.

Что нужно знать об используемой радиостанции:

1. Режим работы: цифровой или аналоговый.
2. Рабочие частоты радиостанции, на которых работает Ваше подразделение.
3. Какие каналы (рабочие частоты) являются основными, какие резервными.
4. Наличие шифрования, кодирования или маскирования.
5. Мощность излучения, возможность её регулировки.

Что необходимо иметь в запасе:

1. **Антенны.** На каждый частотный диапазон необходимо иметь, кроме основной, ещё как минимум одну запасную. Обращайтесь с антеннами аккуратно, не носите радиостанцию держа за антенну, не сгибайте и не проверяйте на прочность. Не включайте радиостанцию на передачу без антенны. Не прикасайтесь к антенне во время передачи.
2. **Аккумуляторы.** На холоде аккумуляторы разряжаются быстрее, поэтому необходимо иметь запас. Не оставляйте аккумуляторы на солнце или рядом с высокочастотной техникой.
3. **Гарнитуры.** Для удобства эксплуатации и повышения эргономики комплексов радиосвязи рекомендуется использовать специальные радиогарнитуры: портативные, шумозащищённые, костной проводимости, для ношения под каской, ларингофонного типа.

Общие выводы по разделу:

1. От грамотного радиопланирования напрямую зависит эффективность работы радиосети.
2. Ответственно относитесь к эксплуатируемому оборудованию, тогда оно прослужит Вам дольше.
3. Запомните основные характеристики используемой радиостанции.

2. ВЕДЕНИЕ ПЕРЕГОВОРОВ

Правила радиообмена необходимо соблюдать с целью избегания задержек, ошибок и обеспечения безопасности радиосвязи. Перед началом радиосеанса прослушайте радиоэфир. Убедитесь, что канал не занят. Для аналогового оборудования необходимо проверить уровень шумов, отключив шумоподавитель (подавитель шума автоматически включается, когда уровень входного сигнала становится меньше определённого порога, т. е. при приёме полезного сигнала повышается уровень порога срабатывания, шумоподавитель включает динамик). Убедитесь, что уровень шумов в канале позволяет производить сеанс связи.

Радиосообщения должны быть четкими, краткими, однозначными, предварительно продумайте радиосообщение. Во время сеанса связи произносите слова чётко, медленно. Если принимающий оператор должен вести запись, оставляйте для этого время.

При радиопереговорах запрещается прерывать ведущийся радиообмен без необходимости, мешать выходу на передачу других подразделений на частотах, не закреплённых за Вашим подразделением, вести переговоры по личным вопросам. Произносите позывные чётко. Следует соблюдать очередность в ведении радиопереговоров.

Вызвать корреспондента можно не более 3-х раз подряд, после чего во избежание помех другим корреспондентам сделать перерыв на 1-2 минуты.

Обозначайте начало и конец радиообмена характерными словами: «Приём», «Внимание», «Конец связи» и т. п.

В целях скрытия от противника истинных наименований и целей при передаче информации необходимо работать с позывными и кодовыми таблицами. Позывные и таблицы необходимо менять не реже 1 раза в неделю (лучше чаще), в том числе для радиостанций с маскиратором и кодированием/шифрованием.

Чтобы не привлекать к себе внимания со стороны противника, используйте обезличенные цифровые позывные (например, «Пятый», «Тридцать шестой» и др.), которые будут меняться.

Для того чтобы позывной можно было легко разобрать в условиях помех и шумов, он должен быть коротким и чётким. Используйте звонкие согласные (Г, Д, Р, З и т.д.) и открытые гласные (А, О, У, И). Позывной должен быть широко используемым словом, с однозначным ударением.

Используйте при радиообмене распознавание «свой/чужой» (пароль и отзыв). Например, с помощью цифровых паролей – «вопрос 456», «ответ 844» (верный). Парольные пары следует использовать однократно.

Общие выводы по разделу:

1. Общение по радиосвязи должно быть кратким, чётким, однозначным.
2. Соблюдайте очередность в ведении радиопереговоров. Не создавайте радиопомех другим подразделениям.
3. Используйте позывные и кодовые таблицы.

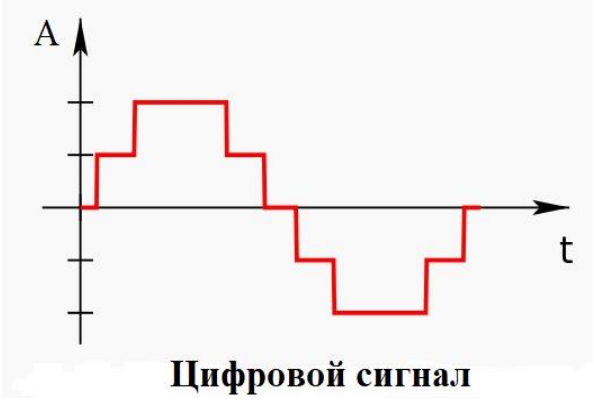
3. ТЕОРИЯ РАДИОСВЯЗИ

3.1 Цифровая и аналоговая связь

Аналоговый сигнал представляет собой непрерывную волну, которая постоянно меняется в течение определенного периода времени. Цифровой сигнал является также непрерывной волной, но которая несет информацию в двоичном формате и имеет дискретные (конечные) значения.

Аналоговый сигнал всегда изображается в виде непрерывной синусоиды, тогда как цифровой сигнал представлен прямоугольными волнами.

Аналоговый сигнал



Цифровой сигнал

Основной тенденцией развития телекоммуникаций во всем мире является цифровизация сетей связи, предусматривающая построение сети на базе цифровых методов передачи и коммутации. Это объясняется следующими существенными преимуществами цифровых методов передачи перед аналоговыми:

высокая помехоустойчивость;

слабая зависимость качества передачи от длины линии связи;

эффективность использования пропускной способности каналов.

В настоящее время на снабжении органов внутренних дел Российской Федерации (ОВД РФ) состоят цифровые и аналоговые радиостанции. По способу распределения абонентов по каналам используются преимущественно конвенциональные и транкинговые системы подвижной связи (СПС).

3.2 Системы подвижной связи

Конвенциональная система связи (КСС) – это система связи (может быть аналоговой, цифровой или смешанной), в которой каждая группа абонентов закрепляется за определенной радиочастотой. Когда одна группа занимает один канал связи, остальные вынуждены ждать, пока он освободится.

Для резервирования радиосвязи (то есть в условиях действия высокого уровня радиопомех или в случаях, когда основная частота скомпрометирована), в радиостанцию «прошиваются» основная и запасная радиочастота. Если, когда отсутствует возможность вести переговоры на основной частоте, абонент может переключиться на запасную. Такие системы используются на территориях с низкой плотностью абонентов. Обычно дальность такой радиосвязи составляет до 2 км, поэтому для увеличения дальности радиосвязи используют ретрансляторы. В зависимости от подвеса антенны ретранслятора радиус действия может достигать 50 – 70 км. На рис. 1, 2 показаны описанные варианты инфраструктуры.

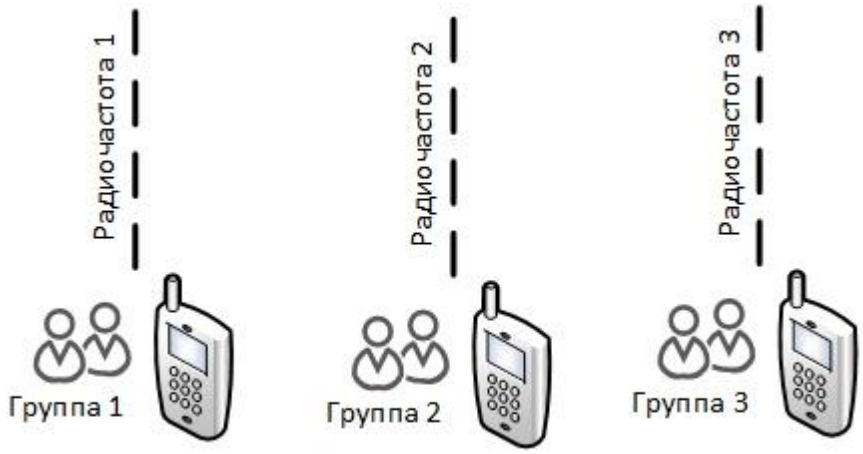


Рис. 1. Пример структуры конвенциональной системы связи

Рис. 2. Пример структуры конвенциональной системы связи с ретранслятором

Транкинговая система связи (ТСС) – это система связи, в которой происходит автоматическое распределение свободных каналов связи между абонентами через базовую станцию. Принцип построения ТСС близок к принципу построения сотовых сетей. Радиообмен осуществляется через базовую станцию (радиосайт), которую устанавливают в центр необходимой зоны обслуживания. Таким образом обеспечивается мобильность абонентов в пределах ограниченной зоны. ТСС с подобной иерархией называют однозоновыми. Несмотря на то, что ТСС возможно развернуть на зону обслуживания, соизмеримую с ячейкой сотовой сети (радиусом до 10 км уверенного приема), сервис абонентов ТСС значительно меньше, чем сервис, предоставляемый сотовой связью. Другая особенность ТСС заключается в максимальной емкости сети (чем больше емкость сети, тем больше абонентов возможно обслуживать одновременно) – у ТСС она значительно ниже.

Структура транкинговой системы представлена на рисунке 3.

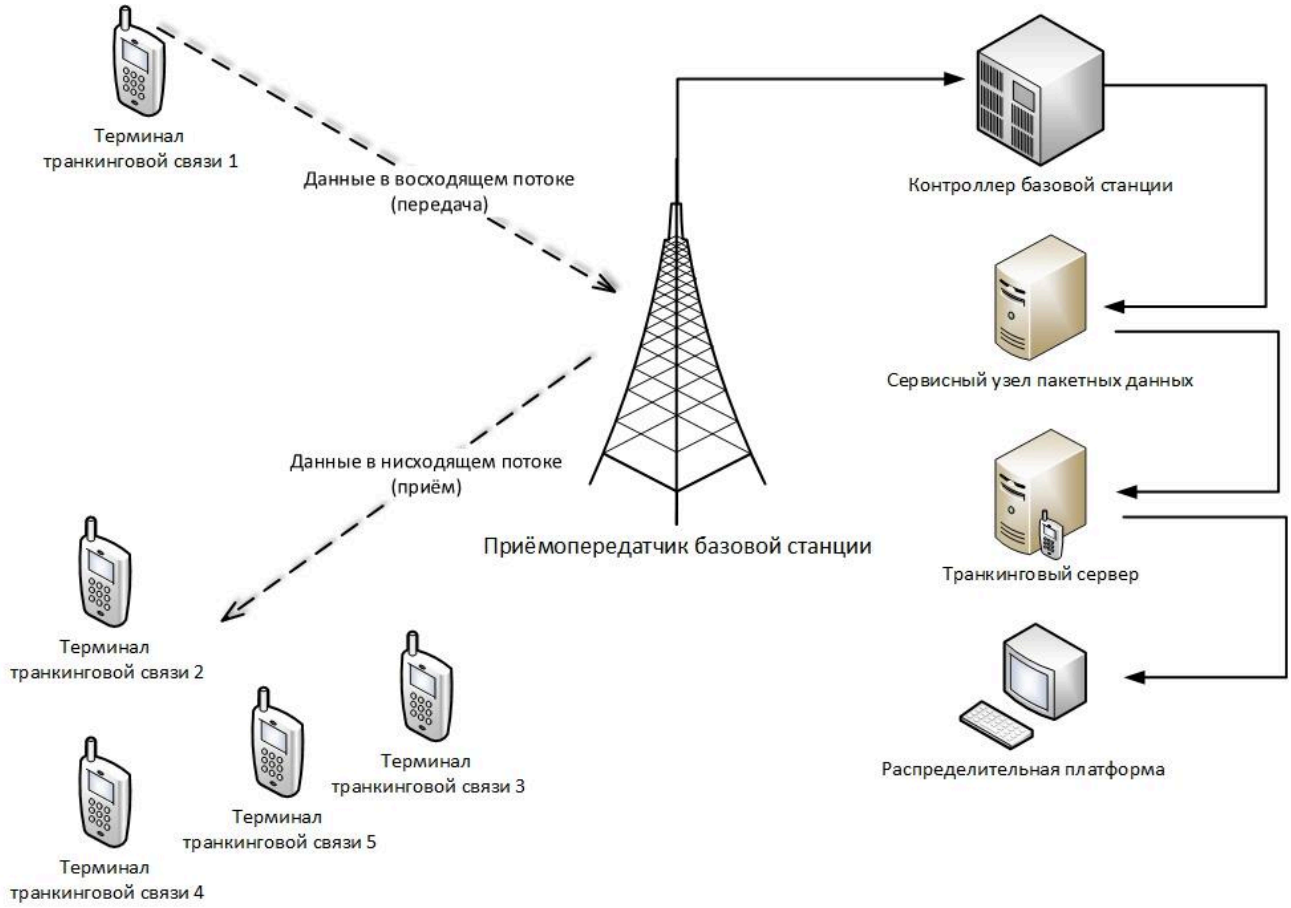


Рис. 3. Пример структуры однозоновой транкинговой системы связи

Для реализации многозоновой ТСС базовые станции комплектуются коммутирующим оборудованием, которое связывается между собой посредством кабельной линии или радиоканалом.

Передающее оборудование в ТСС может быть аналоговым или цифровым. Преимущественно в ТСС используется частотная или фазовая модуляция с шагом сетки частот 12,5 или 25 кГц. Передача речевых сообщений в цифровом оборудовании осуществляется с помощью вокодера, преобразующего аналоговый сигнал.

Общие выводы по разделу:

1. Радиосвязь делится на цифровую и аналоговую. Аналоговая связь прослушивается, поэтому предпочтительно использовать цифровую.
2. В большинстве случаев, системы подвижной связи организуют в виде транкинговой или конвенциональной системы.

4. РЕКОМЕНДАЦИИ ПО ИСПОЛЬЗОВАНИЮ СРЕДСТВ И СИСТЕМ РАДИОСВЯЗИ ОВД РОССИЙСКОЙ ФЕДЕРАЦИИ

В настоящее время на снабжение органов внутренних дел Российской Федерации приняты в подавляющем большинстве узкополосные средства и системы радиосвязи, предназначенные для работы в выделенных МВД России полосах радиочастот П23 (в диапазоне 160 МГц) и П45 (в диапазоне 450 МГц). Частотный диапазон радиостанции, как правило, указан в названии радиостанции.

Почти все используемые радиостанции могут работать как в цифровом, так и в аналоговом режиме. Аналоговая связь прослушивается вся, поэтому общение по аналоговым радиостанциям должно быть минимальным. Изучите руководство по эксплуатации на предмет возможности «переключения» радиостанции на аналоговый и цифровой режим. Обратите внимание на индикацию и символы в строке состояния (если радиостанция имеет экран) при переключении режимов.

Следует отметить, что в настройках цифровых радиостанций, работающих в стандарте DMR, есть возможность дистанционного мониторинга и отключения радиостанцией (по DTMF или kill code). При отключении данной функции противник не сможет дистанционно заблокировать Вашу радиостанцию, но в то же время, если противник завладеет Вашей радиостанцией, то Вы также не сможете удаленно заблокировать её.

ВАЖНО! Всегда по умолчанию считать, что связь прослушивается.

Узкополосные средства и системы, принятые на снабжение ОВД РФ, предназначены для мирного времени, но не для работы в условиях активной радиоразведки и РЭБ противника, поскольку работают на строго определенных частотах, в узких полосах радиочастот (легко подавить), на достаточно большой мощности (легко обнаружить) и не оснащены средствами гарантированной защиты информации (легко перехватить радиопереговоры). Почти все цифровые радиосредства на снабжении ОВД РФ, оснащены так называемыми

маскираторами (преобразователями речевой информации и шифраторами с малой длиной ключа – до 56 бит).

ВАЖНО! Будьте внимательны, маскираторы не гарантируют защищенности от перехвата, они предназначены лишь для того, чтобы информация не прослушивалась на обычном сканере.

В случае использования в условия СВО таких узкополосных средств (когда других не имеется) очень важно соблюдать организационные меры:
не работать на повышенной мощности при работе на небольших расстояниях между точкой приема и точкой передачи (т.е. работа на пониженной мощности). Перед использованием радиостанции изучите руководство эксплуатации на наличие механизмов снижения выходной мощности. Как правило, на радиостанциях либо уже есть заранее запрограммированная кнопка, либо переключение программируется на любую свободную кнопку;
передача должна быть только при необходимости и предельно короткой;
по возможности менять место дислокации при выходе на передачу;
применять сменяемые переговорные таблицы для радиообмена;
при работе в темное время суток отключать любую световую индикацию (как правило, такая настроика возможна при программировании радиостанции).

Более приспособлены к работе в боевых условиях радиостанции «Гранит Р-86АЦ» («Волновая сеть»), принятые на снабжение ОВД РФ. Комплекс цифровой радиосвязи «Волновая сеть» позволяет создать гибкую радиосеть, основой которой является ретрансляция сигнала каждой станцией. То есть сеть представляет собой аналог MESH и MANET-сетей (сети с ячеистой структурой). При передаче радиостанции «Гранит Р-86АЦ» используют сравнительно низкую мощность излучения (0,25 Вт), что даёт в условиях радиопеленгации преимущество перед другими радиостанциями (в среднем мощность радиостанций составляет около 5 Вт).

Комплекс цифровой радиосвязи «Волновая сеть» позволяет создать гибкую радиосеть, основой которой являются узловые радиостанции, связанные со всеми станциями внутри одной сети. Таким образом, при выбывании узла из

топологии (например, из-за неисправности устройства) его соседи могут быстро перестроить маршрут для трафика. Пример организации такой сети представлен на рис. 4:

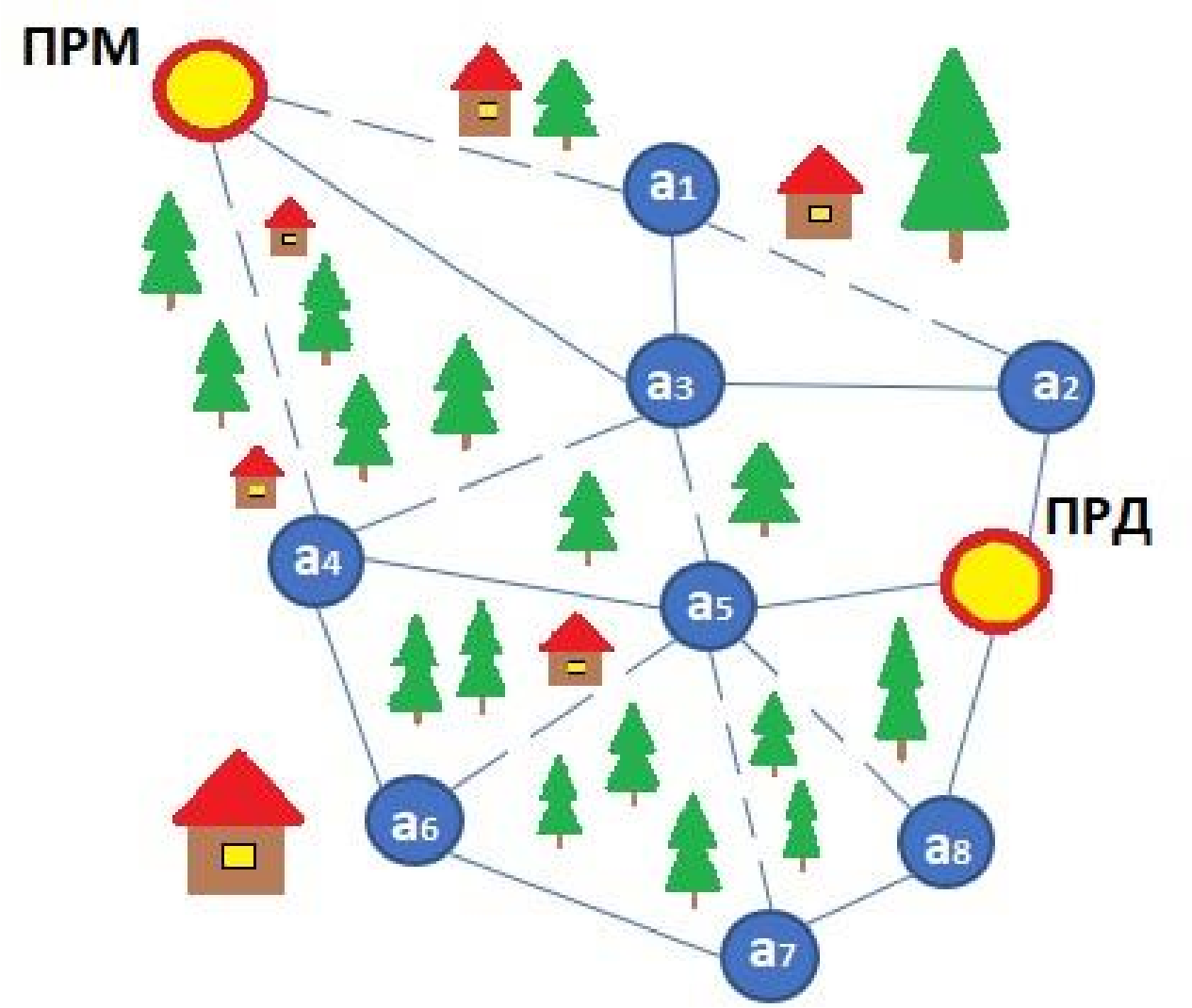


Рис. 4. Пример формирования MESH-сети:
ПРМ – (приёмник) получатель; ПРД – (передатчик) отправитель;
$a_1 – a_8$ – промежуточные узлы

При передаче пакета данных выстраивается маршрут до получателя таким образом, что каждый узел гарантирует дальнейшую передачу пакета. Гарантия передачи обеспечивается регулируемой избыточностью сетевого трафика.

Все переговоры и данные, которыми обмениваются абоненты радиосети, маскируются с помощью алгоритма шифрования с применением короткого ключа. Из перехваченного трафика достаточно трудно получить

информационную составляющую. Каждый канал имеет индивидуальный ключ. В ситуации, когда у противника оказывается радиостанция, необходимо как можно скорее сменить ключ. Смену ключа осуществляет ответственный за радиосвязь сотрудник.

В качестве недостатков такой системы можно отметить высокую задержку доставки сообщений между абонентами, находящимися на максимальном удалении друг от друга. Это связано с тем, что малогабаритные станции работают на небольших дальностях (до 200 м). В условиях сложного рельефа и перепада высот дальность радиосвязи сильно сокращается, буквально до 50 – 100 м. Если Вам необходимо передать информацию на дальнее расстояние, например на несколько десятков километров, то путь радиосигнала через малогабаритные станции займёт несколько секунд. Чтобы ускорить передачу информации на дальние расстояния, старайтесь использовать носимые радиостанции-ретрансляторы дальнего действия (радиостанции Р48У.3, Р48У.8) или специальные ретрансляторы (радиостанции Р48У.9), увеличивающие зону покрытия радиосвязи.

При этом необходимо учитывать, что радиостанции «Гранит Р-86АЦ» всегда находятся в режиме приёма-передачи, а значит могут быть запеленгованы в непосредственной близости от сканера. Радиус пеленга зависит от местности и чувствительности пеленгатора. Чем рельефнее местность, тем больше затухание сигнала. Чем выше чувствительность радиопеленгатора, тем дальше он может сканировать сигнал.

Действуя в боевых условиях, при выборе средств радиосвязи старайтесь соблюдать **баланс** между увеличением зоны покрытия радиосвязи и мощностью излучения. Грамотно расставляйте приоритеты, учитывая цели поставленных боевых задач, уровень подготовки подразделения, рельеф района боевых действий, технические возможности и т. д.

Общие выводы по разделу:

1. Помните, что средства и системы, принятые на снабжение ОВД РФ, предназначены для мирного времени, поэтому при их использовании в

условиях СВО соблюдайте организационные меры.

2. Будьте внимательны: маскираторы и шифраторы, не являющиеся средствами КЗИ, не гарантируют защищенности от перехвата, они предназначены лишь для того, чтобы информация не прослушивалась на обычном сканере.
3. Предпочтительнее использовать более приспособленные к работе в боевых условиях радиостанции «Гранит Р-86АЦ» («Волновая сеть»).

5. УКАЗАНИЯ ПО ИСПОЛЬЗОВАНИЮ МОБИЛЬНЫХ ТЕЛЕФОНОВ

Мобильный телефон – мощный источник информации. Все мобильные телефоны, в том числе кнопочные, предоставляют возможность удалённого определения местоположения абонента, перехвата данных, прослушивания вызовов.

ВАЖНО! Использование мобильного телефона – прямая угроза жизни сотрудников. Категорически запрещается передавать по мобильной связи критически важную информацию!

5.1 Принцип работы

В начале работы, т. е. при включении SIM-карты в телефон, абонент регистрируется в сети с помощью служебных сигналов. Мобильный телефон отправляет сигналы, ждёт ответа от базовой станции (БС) и, если соединение прошло успешно, они обмениваются информацией о местоположении, характеристиками сети (ширина канала, формат канала и т. д.). После того как мобильный телефон и БС завершили коммутацию, по служебному каналу мобильный телефон практически непрерывно сообщает о себе различные данные БС. Это необходимо для того, чтобы БС отслеживала местоположение абонента и готова была выделить канал для вызова или передачи данных. То есть базовая станция непрерывно следит за мобильным устройством. С помощью, записанной в SIM-карте информации в результате взаимного обмена данными между мобильным телефоном и сетью, осуществляется полный цикл аутентификации и разрешается доступ абонента к сети. При движении абонента соседние БС

обмениваются информацией об абоненте и прогнозируют траекторию его дальнейшего передвижения.

Во всех мобильных телефонах встроен специальный чип памяти записывающий все базовые станции, к которым когда-либо присоединялся телефон. Поэтому в зоне СВО ни в коем случае нельзя использовать SIM-карты и телефоны, когда-либо применяемые в России. В противном случае Ваша жизнь и жизнь Ваших близких может быть подвергнута опасности (см. раздел «5.4 Идентификация личности»).

5.2 Мобильный роуминг

Если SIM-карта принадлежит российскому оператору, а Вы находитесь за пределами Российской Федерации, то доступ к звонкам, SMS и другим услугам, предоставляемым операторами связи, будет возможен только если БС иностранного государства подключена к услуге, называемой «роуминг». Эта услуга доступна не во всех регионах, поэтому существует вероятность, что на территории иностранного государства телефон с российской SIM-картой не будет «ловить сеть». Если всё же удалось подключиться к мобильной сети, то принцип коммутации абонента с БС примерно такой же, как и для абонентов внутри страны.

Таким образом, спецслужбы противника имеют полный доступ к сотовым сетям, а значит с помощью специальных технических мер осуществляется полный контроль сотовых сетей на территориях, не принадлежащих Российской Федерации. В первую очередь, спецслужбы выявляют абонентов, которые совершают вызовы в Российскую Федерацию по нумерации (+7 и 8). Следующий шаг – перехват вызова и идентификация личности и/или круга интересов, взаимодействующих лиц, определение местоположения. Противник может использовать данную информацию в нескольких негативных сценариях: морально-психологическое давление на сотрудника или родственников, нанесение огневого удара по месту расположения личного состава и т. д.

ВАЖНО! Известны примеры, когда на границе Российской Федерации с иностранным государством противник подавляет БС российских операторов, тогда мобильный телефон автоматически подключается к ближайшей БС, принадлежащей иностранному государству, и таким образом осуществляется перехват данных. Достаточно нескольких секунд, чтобы при подключении телефона к зарубежной БС противник получил доступ к телефонным номерам и переговорам.

Определить, что телефон находится в международном роуминге, можно по нескольким признакам:

на панели состояния горит соответствующий индикатор;

на панели состояния отображается оператор другой страны;

в настройках сети телефона, во вкладке «данные/Интернет в роуминге» активирована передача данных.

Во избежание демаскирования, необходимо отключить услугу передачи данных в «роумниге». Для этого в настройках телефона найдите раздел «SIM-карты и мобильные сети», далее настройки мобильной сети в роуминге (или расширенные настройки), отключите международный роуминг для всех приложений без исключения.

При включении «Авиарежима» мобильное устройство всё ещё остается в сети, разница лишь в том, что БС не даёт совершать и принимать вызовы, выходить в Интернет. Аналогичная ситуация с выключенным телефоном.

Важно отметить, что все мобильные телефоны и SIM-карты сохраняют всю личную информацию пользователя: сведения о трафике, журнал событий, фото- и видеоматериалы, информацию об онлайн-покупках, телефонные номера и т. д., поэтому в случае крайней необходимости рекомендуется использовать новый телефон и SIM-карту, с которой ранее не совершались звонки на территорию Российской Федерации.

ВАЖНО! При выполнении специальных задач за пределами Российской Федерации или на границе с иностранным государством мобильные телефоны используют БС принадлежащие иностранным государствам, что позволяет спецслужбам производить прослушивание телефонных разговоров сотрудников силовых служб. Полученная информация используется для выявления планов действий/маневров подразделений с целью нанесения огневых ударов.

Защитными мерами в данном случае являются только извлечение из телефона SIM-карты или отключение питания телефона (извлечь аккумулятор).

5.3 Точка доступа (Wi-Fi)

Wi-Fi легко пеленгуется противником (с расстояния от 100 м). Также при его использовании легко определяется количество подключённых к точке доступа абонентов.

ВАЖНО! Использование мобильного телефона в качестве точки доступа (Wi-Fi) категорически запрещено!

При использовании телефона в качестве точки доступа он по сути является ретранслятором трафика с подключенных по Wi-Fi телефонов на базовую станцию, а далее БС распределяет трафик в соответствии с запросом.

Соответственно, активность трафика с телефона, используемого в качестве точки доступа, гораздо выше, мощность излучения максимальная и его легко обнаружить даже бытовым радиопеленгатором. При этом весь трафик идёт через БС. Методы прослушивания через сотовые сети описаны в предыдущем разделе. Так как телефоны связаны между собой, то противник аналогично может прослушивать всю сеть.

5.4 Идентификация личности

Первое, с чего начинается идентификация пользователя мобильного телефона, – это номер телефона. Номер телефона является уникальным идентификатором, по которому можно не только определить регион и оператора

связи, но и получить доступ к мессенджерам, социальным сетям, к телефонной книжке, электронной почте, облачным хранилищам медиафайлов и т. д. Существует большое разнообразие схем, при которых противник может получить доступ к информации, хранящейся на мобильном телефоне. Схемы различаются сложностью и необходимостью технического оснащения.

Один из самых простых способов получения данных для доступа в мессенджер или электронный почтовый ящик – это использование «фишинговых» ссылок. Такие ссылке могут распространяться в прямом виде (т. е. в виде гиперссылки) или с помощью QR-кода. Перейдя по ссылке, Вы увидите копию известного Вам мессенджера или почтового сервиса (например, WhatsApp, Mail.ru, Telegram и т. д.), где Вас попросят авторизоваться, введя логин/номер телефона/почту и пароль. Доступ к ресурсам Вы не получите, а, наоборот, введённые данные противник будет использовать для доступа к Вашим аккаунтам, телефонным книжкам и перепискам. Подобные ссылки могут быть замаскированы под безобидным предложением пройти опрос о качестве обслуживания или получении уникальной скидки.

ВАЖНО! Соблюдайте бдительность при переходе по внешним ссылкам.

Другой способ, требующий технического обеспечения, – перехват пакетов трафика. Как описывалось в предыдущем разделе, если Ваш телефон коммутирован к БС противника, то все пакеты данных (звонки, сообщения, интернет-трафик) идут через противника. С помощью специальных программ можно получить доступ ко всем Интернет-ресурсам, которыми Вы пользовались, а также к паролям и логинам.

Так как весь сотовый трафик находится под контролем специальных служб противника, они владеют ключами от популярных мессенджеров (WhatsApp, Viber), что в ходе проведения комплекса технических мер дает им возможность выявлять сведения различного характера: служебную информацию о позициях/маневрах и боевых задачах, личные и компрометирующие данные сотрудников. Полученная информация используется для нанесения огневых

ударов, морально-психологического давления или шантажа. С помощью специального оборудования спецслужбы могут также записывать голосовую речь для последующей имитации.

В случае, если Ваш мобильный телефон попадёт к противнику, то по сохранённым медиафайлам (фото и видео) и приложениям, например «getcontact», можно идентифицировать личность, а также круг общения. Результатом является морально-психологическое воздействие на близких родственников владельца номера с целью шантажа и давления. Не сообщайте по телефону, в мессенджерах свои геоданные, координаты.

Любой фотоснимок или видеозапись в зоне СВО может содержать информацию, которая может быть проанализирована противником в целях сбора разведывательной информации!

ВАЖНО! Не давайте описаний местности. **Любой фотоснимок или видеозапись, скриншот, закладка в приложении с картами в зоне СВО могут содержать информацию, которая может быть проанализирована противником в целях сбора разведывательной информации! Убедитесь, что используемый телефон не содержит НИКАКОЙ личной и служебной информации (Ваше имя, фамилия, дата рождения, номер машины и т. п.).**

5.5 Мобильные приложения и другие функции

Почти все мобильные приложения требуют разрешение на предоставление личных данных (например, ФИО, номер телефона, e-mail и т. д.) и/или геолокацию. Даже если приложение кажется безобидным, например игра или видеосервис, то стоит отказаться от его установки, потому что, как правило, защита персональных данных там невысокая, а указанные сведения или разрешения могут привести к раскрытию личности или местоположения.

Существуют приложения, которые предоставляют доступ к микрофону или видеокамере телефона. Такие приложения способны работать в фоновом режиме, то есть быть абсолютно незаметными для пользователя. Приложения-

шпионы могут быть занесены на телефон при скачивании файлов или программ, также при посещении непроверенных сайтов. Зараженный вирусом файл самостоятельно устанавливается на мобильном устройстве на базе операционных систем Android/iOS и может транслировать всю имеющуюся информацию в режиме реального времени. Подобные программы способны контролировать смартфон пользователя по расписанию или при необходимости.

Использование фитнес-браслетов, умных часов и других трекеров также ставит под угрозу Вашу жизнь и здоровье. Гаджеты такого рода подключаются через облачное хранилище к мобильному телефону и передают на него информацию о местоположении, совершении вызовов, а также могут записывать аудио- и видеоинформацию. Поэтому использование любой носимой электроники в зоне боевых действий **запрещено**.

Лучше всего отказаться от использования дополнительных гаджетов, посещения ненадёжных Интернет-ресурсов, социальных сетей, установки ненужных приложений и переходов по подозрительным внешним ссылкам, так как подобные действия могут привести к раскрытию личности или служебной информации. Полученные сведения противники могут использовать с целью прямого удара по подразделению, или для шантажа сотрудника, его товарищей или родственников. Не подвергайте опасности себя и Ваших близких. Будьте крайне бдительны и осмотрительны.

Не используйте никаких биометрических данных на разблокировку телефона. Применяйте только цифровые пароли, длиной не менее 6 символов. Не ленитесь ставить стирание информации после неправильно введенного пароля.

Чтобы исключить любую возможность дискредитации работы органов внутренних дел Российской Федерации запрещается использование трофейных мобильных устройств (в том числе кнопочных телефонов, смартфонов, планшетов, умных часов, коммуникаторов, фитнес-браслетов, фотоаппаратов, видеокамер и др.). Такой строгий запрет связан с тем, что даже если внешне устройство кажется новым или безопасным, то это в действительности это может

оказаться совсем не так. Внутри устройства может быть замаскирован так называемый «жучок», мини-камера или взрывное устрйство. Пример встраивания подобного «жучка» показан на рис. 5.

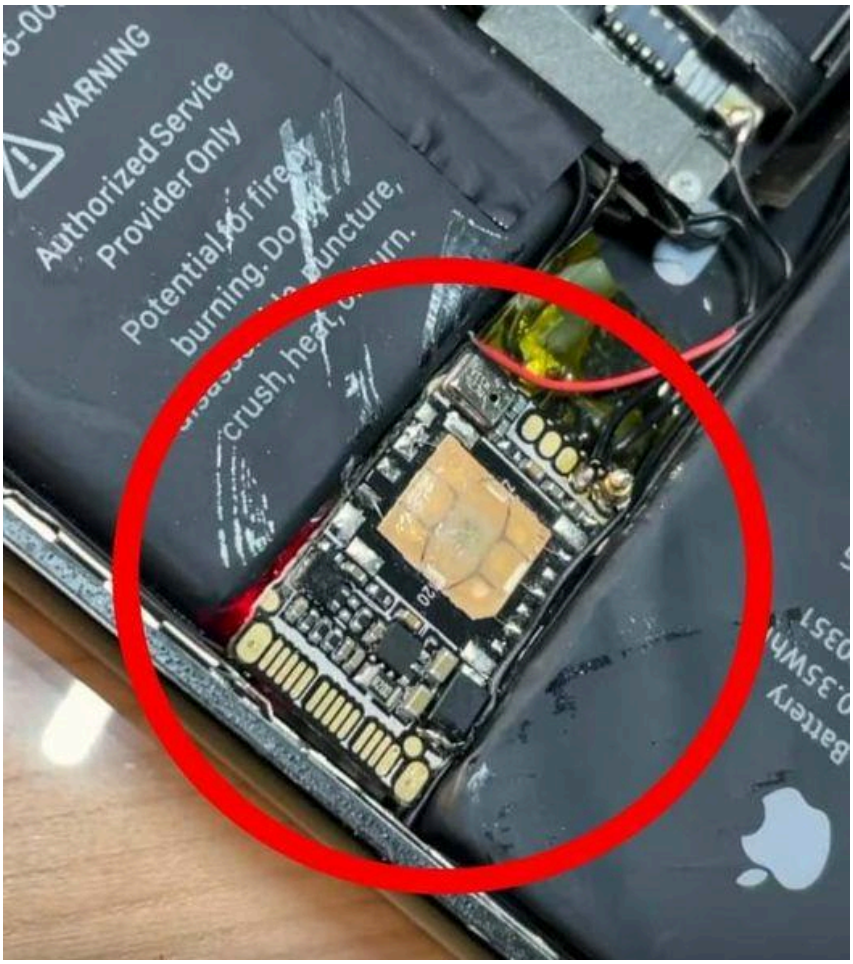


Рис. 5. Пример прослушивающего устройства в трофейном мобильном телефоне

ВАЖНО! При использовании трофейного устройства возможна компрометация служебных или личных сведений, что приводит к огневому удару или морально-психологическому воздействию.

5.6 Рекомендации по ведению сеансов связи с использованием мобильного телефона

При переговорах с использованием мобильного телефона следует руководствоваться теми же правилами ведения переговоров, что и для обычной радиостанции. Запрещается одновременно использовать несколько сотовых устройств, находясь в непосредственной близости (на одной локации). Другими

словами, избегайте скопления абонентских устройств. При одновременном включении нескольких устройств противнику легче запеленговать радиосигнал. Кроме того, разговоры могут быть перехвачены. И, как следствие, – нанесен удар по личному составу. Категорически запрещается совершать и принимать вызовы из мест постоянной дислокации. По завершении сеанса связи необходимо сменить место дислокации.

Сеансы связи должны быть максимально короткими по времени. Рекомендуется использовать закрытые мессенджеры: Telegram, Tukan. Категорически запрещено использование WhatsApp и Viber. Используйте короткие фразы и тексты. При длительном разговоре противник может записать Ваш голос на цифровой носитель для использования в дальнейшем с целью шантажа или распознавания голоса.

Для исключения различных негативных сценариев если Ваш телефон в случае гибели, в плену или при утере попадет в руки к противнику в памяти мобильного устройства запрещается хранить историю вызовов, номера телефонов в открытом виде, любые медиаматериалы и т. д.

Например, по медиаматериалам и истории вызовов противник устанавит Вашу причастность к тем или иным событиям в зоне боевых действий. Существует вероятность, завладев номерам сотрудников, заманить их в засаду или запугивать, оказывать влияние на морально-психологическое состояние.

Номера телефонов рекомендуется хранить в зашифрованном виде. Лучше всего придумать свой способ шифрования, увеличив при этом количество цифр номера не менее чем в 1,5 раза.

Можно приобрести экранирующий излучение чехол для смартфона (по запросу «чехол для смартфона клетка фарадея»), обладающий физическими свойствами Клетки Фарадея. Такие чехлы предназначены для предотвращения прохождения сигнала смартфона, но не дают стопроцентной гарантии от пеленгации.

Общие выводы по разделу:

1. Использование мобильного телефона – прямая угроза жизни сотрудников. Категорически запрещается передавать по мобильной связи критически важную информацию!
2. Не храните в памяти телефона и SIM-карты номера телефонов, фото и видео материалы, личные данные, геопозиционные метки, карты, фото документов и т. д. Не устанавливайте и не пользуйтесь приложениями и мессенджерами. При завладении Вашим телефоном противник может использовать любую информацию против Вас, Ваших родственников и подразделения в целом.
3. Запрещено использование телефона в качестве Wi-Fi точки, не позволяется одновременно включать в одном месте несколько телефонов.
4. Указанные меры затрудняют получение информации с Вашего мобильного телефона, но не исключают этого!

6. ПЕЛЕНГАЦИЯ РАДИОСРЕДСТВ

Пеленгация (также беззапросная, пассивная радиолокация) – это определение направления излучения путём измерения и анализа параметров электромагнитного поля. После излучения и приёма радиолокатором сканирующих сигналов происходит сравнение амплитуд пришедших сигналов по двум угловым направлениям (угол азимута и угол местности). Таким образом вычисляется направление и дальность на излучающий объект.

Примеры общего вида экрана пеленгатора представлены на рис. 6-7:

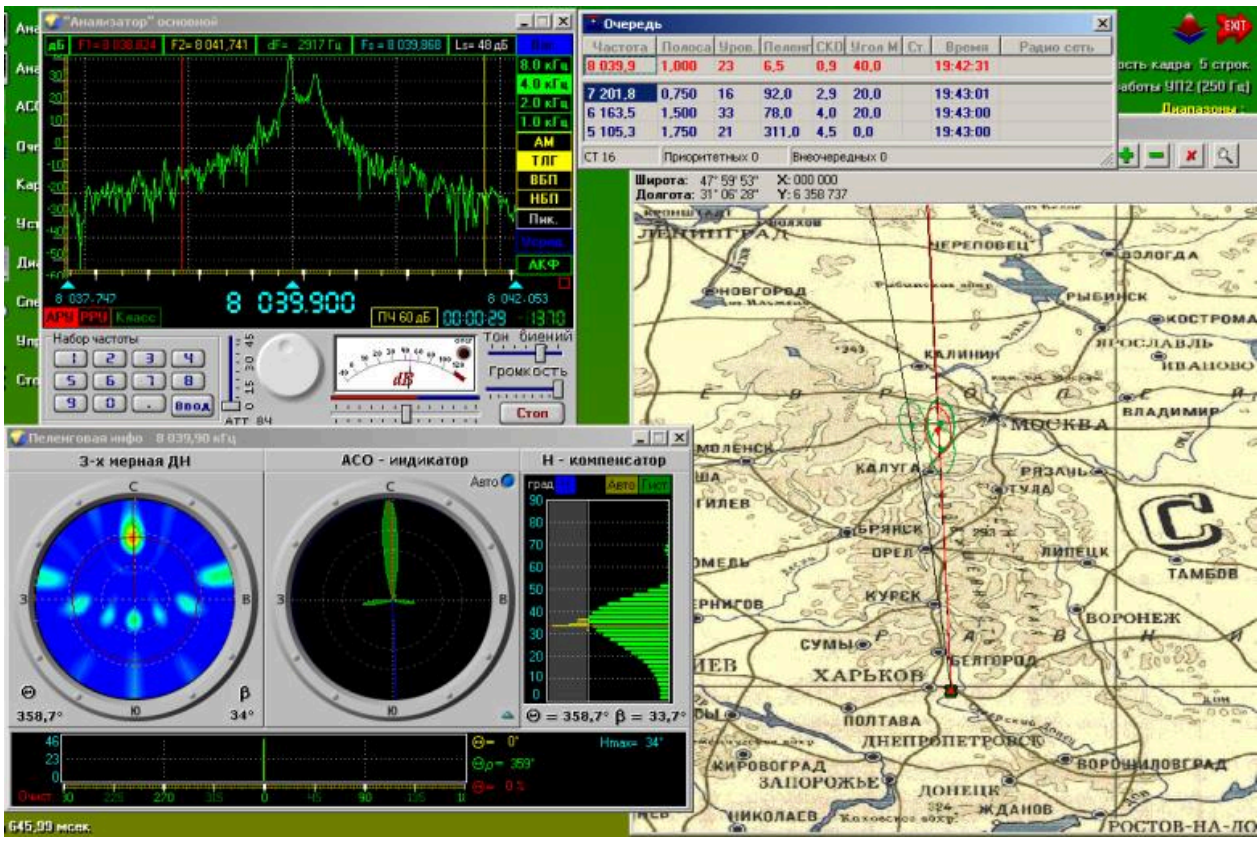


Рис. 6. Пример интерфейса радиопеленгатора

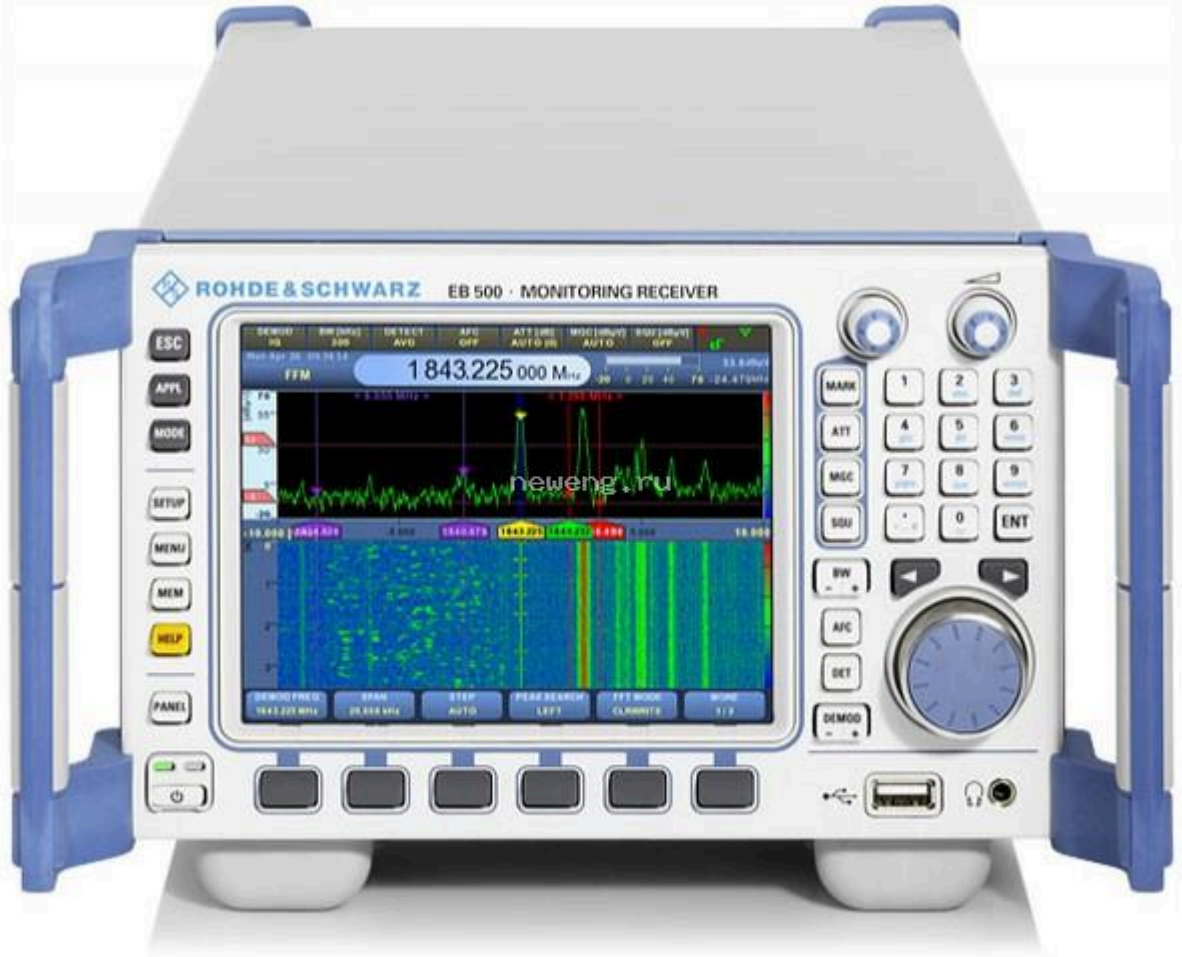


Рис. 7. Пример интерфейса радиопеленгатора

Большее количество измерений дает большую выборку, что повышает точность измерений. Общенациональные пеленгаторы способны обнаружить излучатель с точностью до нескольких сотен метров посредствам триангуляции (т. е. измерения одного и того же параметра несколькими методами). Пеленгаторы, установленные на подвижных средствах, позволяют уточнить местоположение излучателя. Портативные пеленгаторы сужают круг поиска излучателя до нескольких метров.

Эффективность систем радиопеленгации определяется двумя основными параметрами – чувствительностью и помехоустойчивостью. В большей степени определяют эти характеристики антенны, на которых работают радиопеленгаторы. Для разных частотных диапазонов одни и те же средства радиопеленгации не будут одинаково эффективны. На рис. 8 представлены часто используемые современные пеленгаторы для разных частотных диапазонов.

Рис. 8. Примеры внешнего вида антенных устройств средств РЭБ

Самым безопасным видом связи в полевых условиях считаются проводные телефонные аппараты (например, телефон полевой ТА-57). Проводная связь прослушивается только при условии подключения непосредственно к проводной линии и не обнаруживается средствами радиоразведки.

6.1 Рекомендации по радиообмену в условиях пеленгации

Для ухудшения условий радиопеленгации рекомендуется работать на минимальной мощности, так как чем больше мощность Вашей радиостанции, тем легче противнику Вас пеленговать. В радиостанциях предусмотрены режимы Hi (Hi power) и Low (L) (Low power), которые могут быть выбраны путем переключения. Если собеседник находится на небольшом удалении (50 – 500 метров), осуществляйте передачу на малой мощности, т. е. (Low). Обычно режимы Hi и Low выбираются запрограммированной кнопкой на клавиатуре радиостанции (при этом на экране может отображаться буква L или H).

Рис.9. Отображение пониженной и повышенной мощности на экране радиостанции

Вторая рекомендация заключается в использовании коротких речевых сообщений. Чем дольше радиостанция в эфире (т. е. работает на передачу), тем проще пеленговать. По умолчанию – радиостанция пеленгуется за секунду, если противник настроен на эту частоту. Радиостанции, настроенные **только** на приём, не пеленгуются.

ВАЖНО! Применение данных способов для мобильного телефона не помогут: базовые станции все равно его запеленгуют.

Будьте внимательны! Учитывайте, что радиостанции, работающие в

режиме ретрансляции (т. е. в режиме приема-передачи), например радиостанции «Волновая сеть», могут быть запеленгованы, если находятся в непосредственной близости от радиопеленгатора. Также в случае использования транкинговых сетей рации периодически связываются с базой, а значит в этот момент тоже могут быть запелегованы.

При радиообмене необходимо, чтобы до пеленгатора противника сигнал доходил как можно хуже. Это можно обеспечить несколькими способами.

Станцию при разговоре держать параллельно земле и так, чтобы антенна была перпендикулярна тому месту, где находится абонент, с которым вы связываетесь. Отметим, что такое расположение эффективно только на небольших расстояниях между абонентами. Такой способ эффективен, если вызываемые корреспонденты находятся слева и/или справа от Вас. На рисунках ниже схематически представлено распространение радиоволн от рации и наглядная инструкция описанного положения радиостанции.

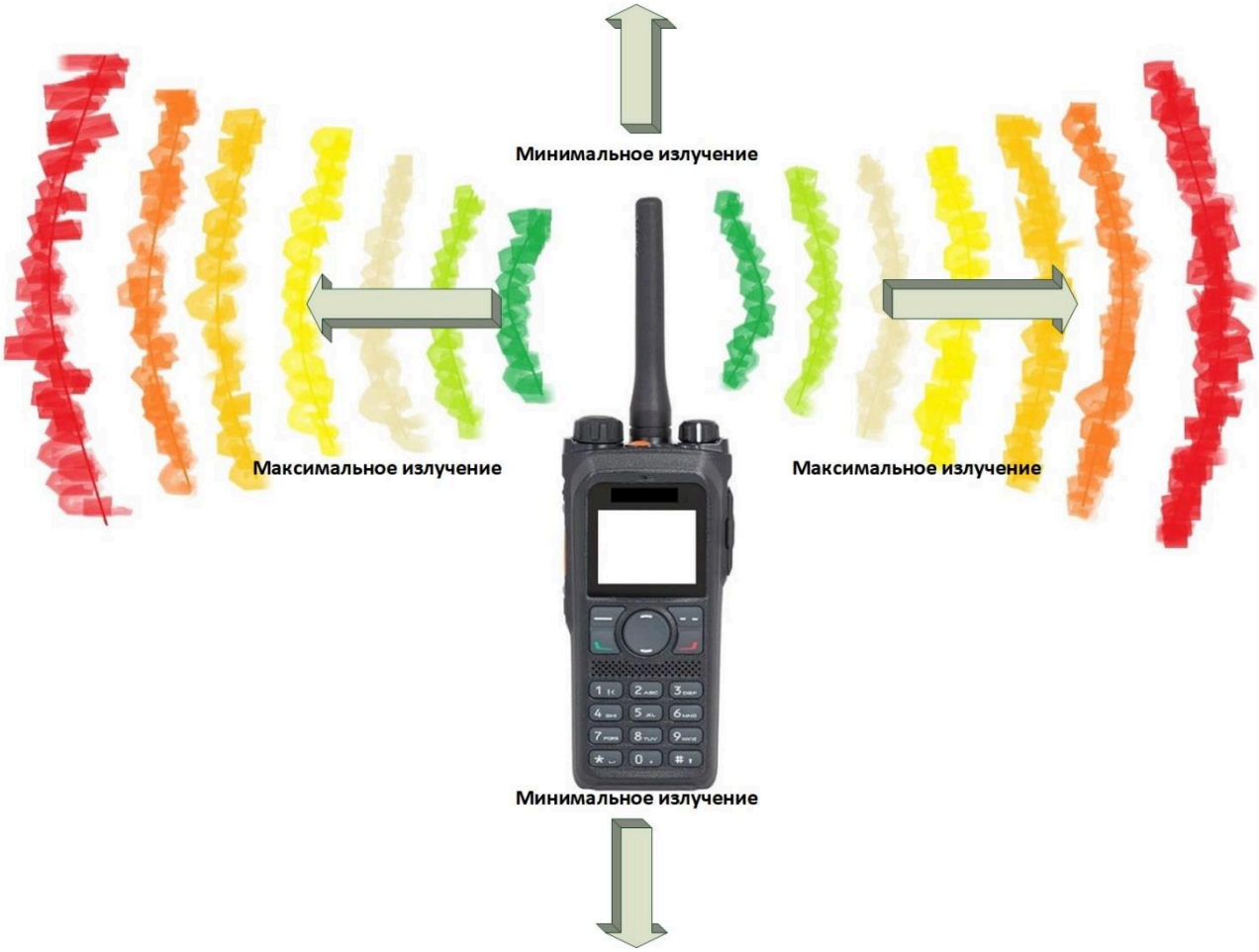


Рис. 10. Визуализация диаграммы направленности носимой радиостанции

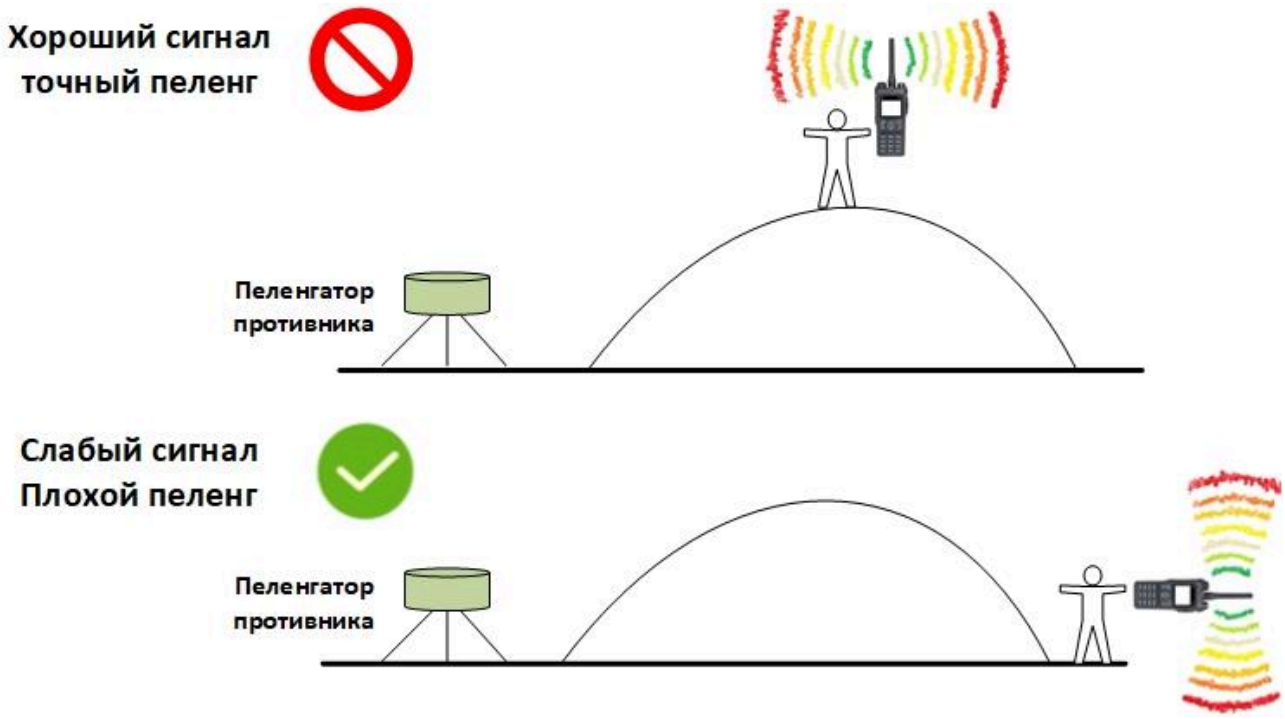


Рис.11. Рекомендуемое использование радиостанции в условиях пеленгации

Используйте обратные скаты высот (между Вами и противником должен быть холм, горка). Используйте препятствия в виде железобетонных конструкций, броню танка, БТР, дверь машины, рельеф местности. Чем больше толщина и площадь препятствия, тем лучше. Старайтесь находиться как можно ближе к экранирующей конструкции, закрываясь ей от линии фронта. Металлические конструкции (даже имеющие полости и отверстия) способствуют отражению радиоволн, а бетонные, земляные конструкции, лесные массивы поглощают радиоволны. Поэтому при использовании металлического экрана, важно размещать его таким образом, чтобы не было переотражения радиосигнала в сторону противника.

Пример использования экранирующей конструкции представлен на рис. 12,13:

Рис. 12. Пример использования экранирующих конструкций (экран)

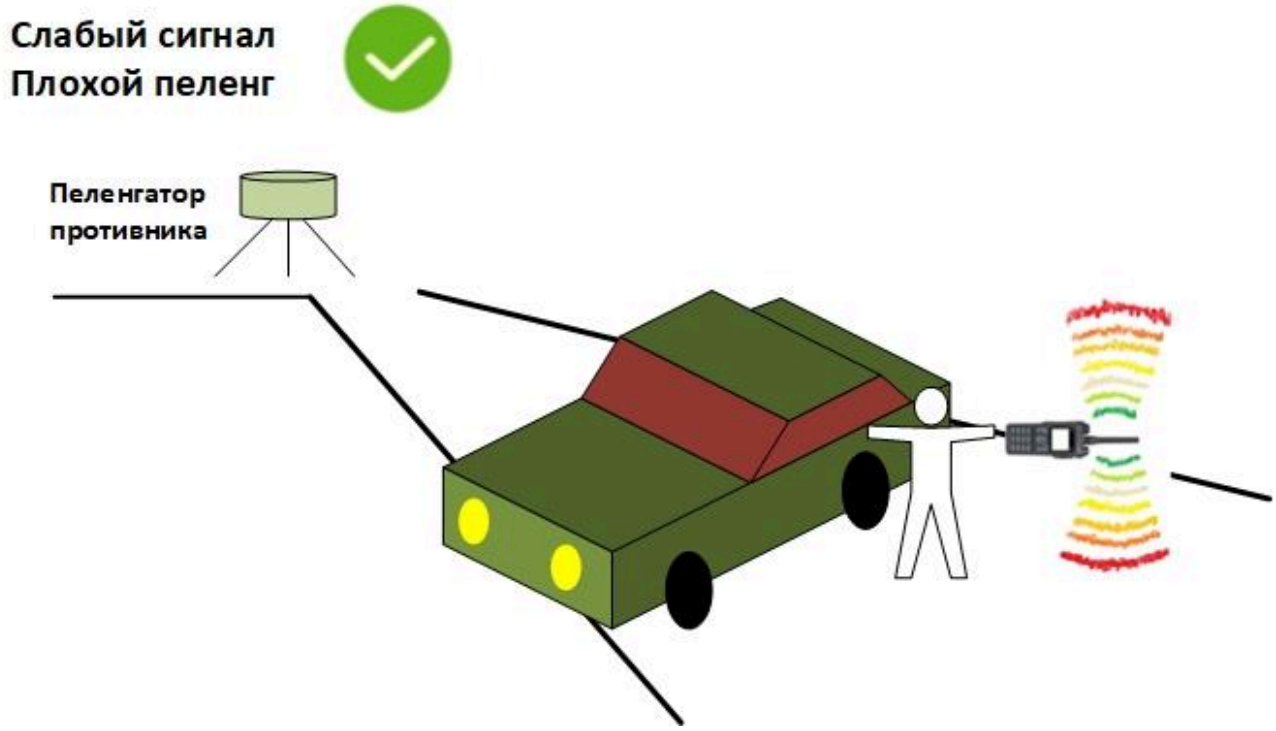


Рисунок 13 – Пример по использования экранирующих конструкций (транспортное средство)

Также рекомендуется использовать станцию-приманку. Для этого необходимо настроить одну станцию на свои частоты и предупредить личный состав, чтобы не реагировали на этот позывной, когда станция будет выходить в эфир. Используйте особый позывной, доклад в виде кодовой таблицы. Доклад осуществляет ответственный за мероприятие. Придайте радиообмену внешнюю важность. Можно использовать аналоговую станцию, приделав к ней длинную (более 100 м) линию (удалённую гарнитуру). По возможности защитить станцию куском бетона, бронепластиной и т. п. Поставить её на относительной

возвышенности, но без возможности для противника визуально (с помощью бинокля, дрона) понять, что там ничего нет. Задача – внушить противнику, что это важный абонент, заставить работать по пеленгации и уничтожению этой станции. Периодически менять это место.

Общие выводы по разделу:

1. Чтобы минимизировать вероятность быть запеленгованным старайтесь использовать минимальную мощность передачи сигнала и максимально короткие сообщения.
2. Периодически меняйте каналы радиосвязи.
3. Используйте рельеф местности и подручные средства для защиты от пеленгации.

7. РЕКОМЕНДАЦИИ ПО УВЕЛИЧЕНИЮ ДАЛЬНОСТИ РАДИОСВЯЗИ

Малая дальность радиосвязи может быть следствием ряда различных причин. Самый вероятные из них – неисправность антенного устройства, помехи в эфире, затенение рельефом. Предварительно изучите руководство по эксплуатации Вашего радиосредства. Правильная эксплуатация решает 80% проблем. Далее приведены методы увеличения дальности связи между радиостанциями:

1. Использование более эффективных антенн. Замена штатной антенны на более эффективную может увеличить дальность радиосвязи на 30%.

Если Ваша антенна пришла в негодность, то выбирайте антенну максимально похожую по характеристикам на штатную. Если есть возможность заменить штатную антенну на более эффективную, то при её выборе обращайте внимание на следующие паспортные характеристики:

полоса частот – она должна совпадать с полосой, в которой работает ваша радиостанция;

коэффициент усиления антенны – чем он больше, тем лучше. При больших коэффициентах усиления возможна работа на пониженной мощности передатчика;

волновое сопротивление – для большинства радиостанций эта характеристика составляет 50 Ом;

коэффициент стоячей волны (КСВ) – характеризует степень согласованности с передатчиком. Чем меньше значение КСВ, тем более антенна эффективна. Идеальный КСВ=1 (т.е. меньше 1 КСВ быть не может), оптимальный для практического применения КСВ не более 2;

поляризация антенны – направленность вектора поля. Как правило, антенны UHF и VHF диапазонов имею вертикальную поляризацию. Старайтесь не использовать антенны с круговой поляризацией;

диаграмма направленности – направленные или всенаправленные.

Максимальное увеличение дальности радиосвязи можно получить, если подключить автомобильную, базовую или коллинеарную антенну. Подключение осуществляется радиочастотным кабелем, допустимая мощность которого не должна быть меньше мощности передатчика. Во время манипуляций по замене антенн запрещается касаться центрального контакта на антенном разъеме и включать радиостанцию в работу.

2. Подъём антенны до условий прямой видимости. Прямая видимость обеспечит максимальную дальность связи. Для маломощных радиостанций это один из самых эффективных способов увеличения дальности радиосвязи. Чтобы обеспечить уверенный приём радиосигнала, необходимо свести к минимуму естественные и искусственные препятствия на пути распространения радиосигнала. Также при работе в условиях радиотени рекомендуется поворачиваться в направлении корреспондента, которому передаётся сигнал.

В случае необходимости размещения радиостанции на теле, не закрывайте антенну телом. Закрепите антенну в верхней части тела, на груди или спине. На рис. 14-15 представлены примеры правильного размещения радиостанции:

Рис. 14. Размещение радиостанции на груди

Рис. 15. Размещение радиостанции на спине

3. Увеличение количества ретрансляторов. Промежуточный ретранслятор увеличит дальность радиосвязи практически в два раза. Более эффективный способ – создание сети из ретрансляторов (например, «Волновая сеть», см. п. 4

«Рекомендации по использованию средств и систем связи ОВД Российской Федерации»). В данном случае возможно реализовать большую зону покрытия. Для увеличения зоны покрытия ретранслятор лучше всего располагать на возвышенности (на холмах, крышах зданий). В некоторых случаях, можно поднять ретранслятор на беспилотным воздушным судном.

Общие выводы по разделу:

1. Правильная эксплуатация оборудования решает большинство проблем, ограничивающих дальность радиосвязи.
2. Три основных механизма, увеличивающие дальность радиосвязи: замена антенны; подъем антенны; увеличение количества ретрансляторов.