

УДК 621.391

## Адресное пеленгование базовых станций GSM, UMTS, LTE сетей сотовой связи

Манелис В. Б., Сладких В. А., Козьмин В. А., Бизюков П. Е.

**Постановка задачи:** Сотовые сети европейских цифровых стандартов GSM, UMTS, LTE пользуются большой популярностью в России и других странах. Необходимость выявления несанкционированно работающих базовых станций (БС) данных сетей, проверки соблюдения частотно-территориального плана, проверки отклонения местоположения БС от условий выданных разрешений требует для операторов и служб радиоконтроля инструментов анализа сигналов БС, включая их пеленгование и оценку местоположения. Множество БС сотовых сетей, характеризующихся своими идентификационными параметрами, осуществляют одновременную передачу в одном частотном диапазоне и оказывают мешающее влияние друг на друга. Это делает невозможным применение фазоразностных способов пеленгования с непосредственным вычислением пеленга и требует разработки новых способов совместной идентификации, пеленгования и оценки местоположения БС. **Целью работы** является разработка способа совместной идентификации и пеленгования обнаруженных базовых станций GSM, UMTS, LTE сетей сотовой связи. **Новизна:** представлен способ радиоконтроля, реализующий функцию адресного пеленгования базовых станций GSM, UMTS, LTE сетей. При этом по принятой реализации сигнала осуществляется одновременная идентификация и пеленгование всех обнаруженных БС. Реализация представленного способа основана на использовании анализаторов БС, включает двухканальный радиоприемник с аппаратурой навигации и антенную решетку. Анализаторы реализуют «адресность», а двухканальный приемник и антенная решетка – пеленгование обнаруженных БС с привязкой к их идентификаторам. **Результат:** предложенный способ адресного пеленгования, использующий информацию о тонкой структуре сигналов БС, позволяет выполнить обнаружение и идентификацию всех обнаруженных БС и сформировать оценку направления на эти БС. Разработанный способ пеленгования внедрен и успешно апробирован в аппаратно-программном комплексе пеленгования сигналов базовых станций на базе пеленгатора АРТИКУЛ-М. **Практическая значимость:** использование адресного пеленгования БС сотовых систем увеличивает функциональные возможности существующих анализаторов сотовых систем связи и позволяет осуществлять определение местоположения базовых станций.

**Ключевые слова:** GSM, UMTS, LTE, базовая станция, анализатор сигнала, идентификационные параметры, адресное пеленгование.

### Введение

Для планирования и эксплуатации сотовых сетей, проверки соответствия требований к параметрам передатчиков, анализа зон покрытия, решения вопросов электромагнитной совместимости необходимо регулярно проводить анализ радиосигналов базовых станций (БС) этих сетей. В [1-6] представлена реализация российских анализаторов сигналов базовых станций сетей GSM (Global System for Mobile Communications), UMTS (Universal Mobile Telecommunications System), LTE (Long-Term Evolution).

#### Библиографическая ссылка на статью:

Манелис В. Б., Сладких В. А., Козьмин В. А., Бизюков П. Е. Адресное пеленгование базовых станций GSM, UMTS, LTE сетей сотовой связи // Системы управления, связи и безопасности. 2021. № 2. С. 142-158. DOI: 10.24412/2410-9916-2021-2-142-158.

#### Reference for citation:

Manelis V. B., Sladkikh V. A., Kozmin V. A., Bizyukov P. E. Base station address direction finding of GSM, UMTS, LTE cellular networks. *Systems of Control, Communication and Security*, 2021, no. 2, pp. 142-158 (in Russian). DOI: 10.24412/2410-9916-2021-2-142-158.

Кроме обнаружения и идентификации актуальной является также задача пеленгования и оценки местоположения БС, решение которой позволяет службам радиоконтроля выявлять несанкционированно работающие БС, проверять отклонение местоположения БС от условий выданных разрешений, осуществлять проверку соблюдения частотно-территориального плана.

Для решения задачи местоопределения базовых станций наиболее эффективным является использование мобильных станций радиоконтроля. Это обусловлено большим количеством БС и их высокой плотностью расположения, особенно в городских условиях. В разных точках траектории движения выполняется обнаружение некоторого количества БС, их идентификация и формирование пеленга (адресное пеленгование). По совокупности пеленгов каждой из обнаруженных БС со своими идентификационными параметрами выполняется расчет их местоположения.

Заметим, что в большинстве сотовых систем связи, в частности, UMTS и LTE, множество БС сети, характеризующихся своими идентификационными параметрами, осуществляют одновременную передачу в одном частотном диапазоне. Это делает принципиально невозможным применение фазоразностного метода пеленгования с непосредственным вычислением пеленга [4-6] и требует выделения сигнала каждой обнаруженной БС из суммарного группового сигнала.

Некоторые способы многосигнальной классификации и пеленгования представлены в [7-9]. В данных работах рассмотрены два разных подхода: метод формирования диаграммы направленности для адаптивных антенных решеток, а также метод, основанный на разделении подпространств сигнала и шума. Последний активно применяется в методах высокого разрешения MUSIC, Root-MUSIC, ESPRIT, а также их модификациях для различных типов антенных решеток, обеспечивающих нужное быстродействие. Практически для всех этих методов требуется предварительная оценка количества сигналов, которая, как правило, априори неизвестна. Указанные методы являются обобщенными и подходят для пеленгования неизвестных сигналов, перекрывающихся по времени и частоте, но они не используют информацию о структуре сигналов пеленгуемых источников и не обеспечивают привязку пеленгов к идентификаторам систем сотовой связи.

В работах [10-12] рассмотрена задача пеленгования абонентских станций системы UMTS на основе разделения подпространств. Предварительно выделяется сигнал каждого абонента, имеющего индивидуальный скремблирующий код, известный на БС. При этом пеленгованию сигнала абонента предшествует вычитание сигналов других абонентов из суммарного группового сигнала. Предложенный метод используется в антенных решетках базовых станций для передачи сигнала в направлении выделенного абонента и реализация данного метода пеленгования возможна только на БС.

В [13, 14] описаны способы оценки направления на БС LTE, основанные на применении антенной решетки абонентской станции и для повышения качества связи абонентской станции посредством формирования максимума диаграммы направленности в направлении мощной БС и подавления сигналов ме-

шающих БС. Определение направления на БС основано на обработке автокорреляционных функций сигналов синхронизации LTE.

В [15] предлагается использование подвижного пеленгатора с фазированной антенной решеткой. Пеленгование базовых станций основано на анализе пиков корреляционных функций общих опорных сигналов. Кроме того, определяется наличие прямой видимости источника. Предлагаемый способ пеленгования позволяет разделять направления прихода сигнала нескольких БС LTE, однако не обеспечивает адресности пеленгования, то есть получения идентификаторов системного уровня.

В данной работе представлен способ радиоконтроля, реализующий функцию адресного пеленгования базовых станций GSM, UMTS, LTE сетей. Его реализация основана на использовании анализаторов БС этих сетей, включает двухканальный радиоприемник с аппаратурой навигации и антенную решетку (АР). Анализаторы реализуют «адресность», а двухканальность приемника и антенная решетка – пеленгование обнаруженных БС.

Работа анализаторов сигналов БС подробно излагалась в [1-6]. В данной статье будет рассмотрен способ совместной идентификации и пеленгования БС сотовых сетей связи, а также особенности адресного пеленгования сигналов БС GSM, UMTS, LTE сетей.

### Общая процедура пеленгования БС сотовых систем связи

Пеленгатор БС сотовых систем связи построен на базе двухканальной приемной аппаратуры пеленгования, использующей многоэлементную антенную решетку. Обозначим номера каналов приемника – 0 (опорный канал) и 1 (сигнальный канал), номера элементов АР –  $m = \overline{0, M-1}$ ,  $M$  – число элементов АР.

Исходными данными для пеленгования являются синхронно поступающие от аппаратуры отсчеты комплексного видеосигнала каждого канала обработки. Комплексный видеосигнал опорного канала 0  $x_{0i}$ ,  $i = \overline{0, N-1}$ , формируется с помощью аналогового тракта, который постоянно подключен к нулевому элементу АР  $m = 0$ . Величина  $N$  представляет собой размер входного блока данных для выбранной частоты дискретизации и зависит от длительности процедуры пеленгования. Комплексный видеосигнал сигнального канала 1  $x_{1i}^{(m)}$ ,  $i = \overline{0, N-1}$ ,  $m = \overline{0, M-1}$ , формируется с помощью аналогового тракта, который последовательно подключается ко всем элементам АР.

На рис. 1 показаны блоки отсчетов сигнала элементов АР  $m = \overline{0, M-1}$  для сигнального тракта и соответствующие блоки отсчетов видеосигнала опорного тракта. Цикл пеленгования занимает интервал времени, в течение которого формируются блоки отсчетов всех элементов АР. Пауза между блоками отсчетов обусловлена временем переключения канала 1 между элементами АР.

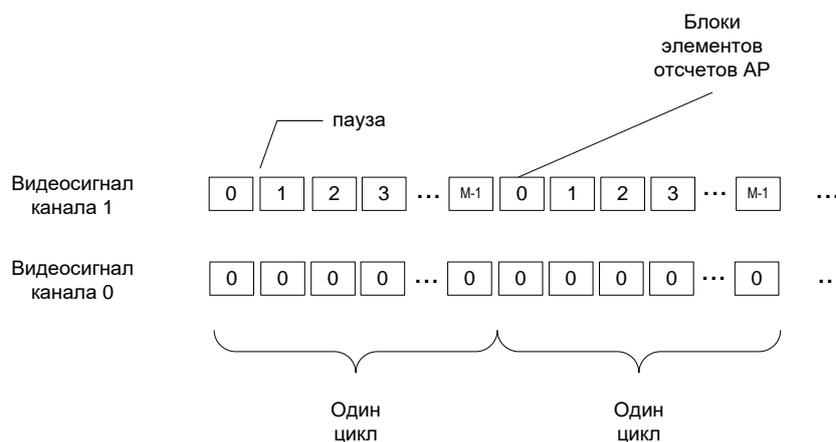


Рис. 1. Временная схема работы пеленгатора

Для каждого цикла пеленгования формируются величины  $U_m$ ,  $m = \overline{0, M-1}$ , которые представляют собой оценку разности фаз между сигналами блоков  $m$ -го и нулевого элементов AP. По величинам  $U_m$  в соответствии с фазоразностным методом пеленгования формируется решающая функция

$$\Omega(\theta) = D(\theta) |\mathbf{U}^T \cdot \mathbf{a}| = D(\theta) \sum_{m=0}^{M-1} U_m \cdot a_m, \quad (1)$$

где  $\mathbf{U}^T = (U_0, \dots, U_{M-1})$ ,  $\mathbf{a} = \left\{ \exp\left( j \cdot \frac{2\pi}{\lambda} \cdot d_m(\theta) \right), m = \overline{0, M-1} \right\}$  – вектор предполагаемых разностей фаз между сигналами  $m$ -ого и нулевого элементов AP в случае угла прихода  $\theta$ ,  $D(\theta)$  – диаграмма направленности элемента AP,  $d_m = ((x_m - x_0) \sin \theta + (y_m - y_0) \cos \theta)$  – разность хода между  $m$ -ым и нулевым элементами AP,  $x_m, y_m, m = \overline{0, M-1}$  – координаты элементов AP,  $\lambda$  – длина волны сигнала.

Оценка направления прихода сигнала (пеленг) определяется по положению максимума решающей функции с учетом угла ориентации AP  $\varphi$ :

$$\tilde{\theta} = \max_{\theta} \Omega(\theta) + \varphi. \quad (2)$$

Каждый отдельный пеленг является случайным и может существенно отличаться от истинного направления на БС ввиду следующих факторов: переотражения сигнала при распространении, особенно, в городской среде, воздействия помех, неоптимального соответствия размеров AP длине волны сигнала БС. Поэтому для повышения помехоустойчивости в каждой точке анализа выполняется некоторое количество циклов пеленгования. Совокупность полученных пеленгов образуют гистограмму пеленгования. Решение о направлении на БС принимается, например, по ее максимуму. Такая оценка оказывается существенно более точной по сравнению с отдельными пеленгами.

Функциональные возможности анализаторов БС реализуются по непрерывному сигналу опорного канала 0. В [1-3] приведены блок-схемы и описание процедур приема, обработки и выделения идентификационных параметров сигналов для каждого из рассматриваемых стандартов сотовой связи.

Формирование оценок разности фаз  $U_m$  (1), используемых для расчета пеленга, имеет свои особенности для каждого из рассматриваемых стандартов.

### Пеленгование БС GSM

Базовые станции GSM сетей включают в общем случае несколько сот, осуществляющих независимую передачу и прием в рамках своего углового сектора. Каждой соте назначается некоторое количество частотных каналов, при этом расположение БС выбирается так, чтобы в зоне обслуживания одной станции не было других станций, работающих на той же частоте. В результате необходимость разделения сигналов БС на одной несущей частоте отсутствует. Однако привязка получаемых пеленгов к БС с соответствующими идентификаторами необходима.

Исходными данными для пеленгования являются два комплексных видеосигнала  $x_{0i}$ ,  $x_{1i}^{(m)}$ ,  $i = \overline{0, N-1}$  с частотой дискретизации  $f_s = 4f_c$ , где  $f_c = 270,83$  кГц – частота следования символов, полоса сигнала 200 кГц. Длина блока отсчетов видеосигнала для каждого элемента АР выбрана 1 мс.

Оценка разности фаз между сигналами блоков  $m$ -го и нулевого элементов АР формируется по формуле

$$U_m = \sum_i x_{1i}^{(m)} \cdot x_{0i}^* . \quad (3)$$

В (3) суммирование выполняется только по отсчетам пакетов символов, отсчеты защитных интервалов пакетов не включаются.

### Пеленгование БС UMTS

Основой технологии UMTS является принцип кодового разделения каналов [2, 3]. Сигналы различных сот сети и различные каналы каждой соты передаются одновременно в одном спектральном диапазоне. При этом каждая сота имеет свой индивидуальный скремблирующий код, позволяющий приемнику выделить сигнал именно этой соты. Для разделения различных физических каналов соты применяются ортогональные канальные коды.

Исходными данными для пеленгования являются два комплексных видеосигнала  $x_{0i}$ ,  $x_{1i}^{(m)}$ ,  $i = \overline{0, N-1}$  с частотой дискретизации  $f_s = 2f_c$ , где  $f_c = 3,84$  МГц – чиповая скорость сигнала UMTS, полоса сигнала 4,25 МГц. Длина блока отсчетов видеосигнала для каждого элемента АР выбрана приблизительно 550 мкс, что соответствует не менее  $512 \cdot 4 = 2048$  чипов. Поскольку переключение сигнального канала между элементами АР не синхронизировано с временной структурой UMTS сигнала, это обеспечивает для каждого элемента АР не менее трех блоков по 512 чипов, для которых анализатор формирует оценку канала.

Последовательность обработки UMTS сигнала при пеленговании представлена на рис. 2. Непрерывный комплексный видеосигнал опорного канала обрабатывается в соответствии с процедурами, описанными в [2, 3]. Среди этих процедур обнаружение базовых станций (сот), временная и частотная синхро-

низация, получение скремблирующих последовательностей и определение числа передающих антенн БС.

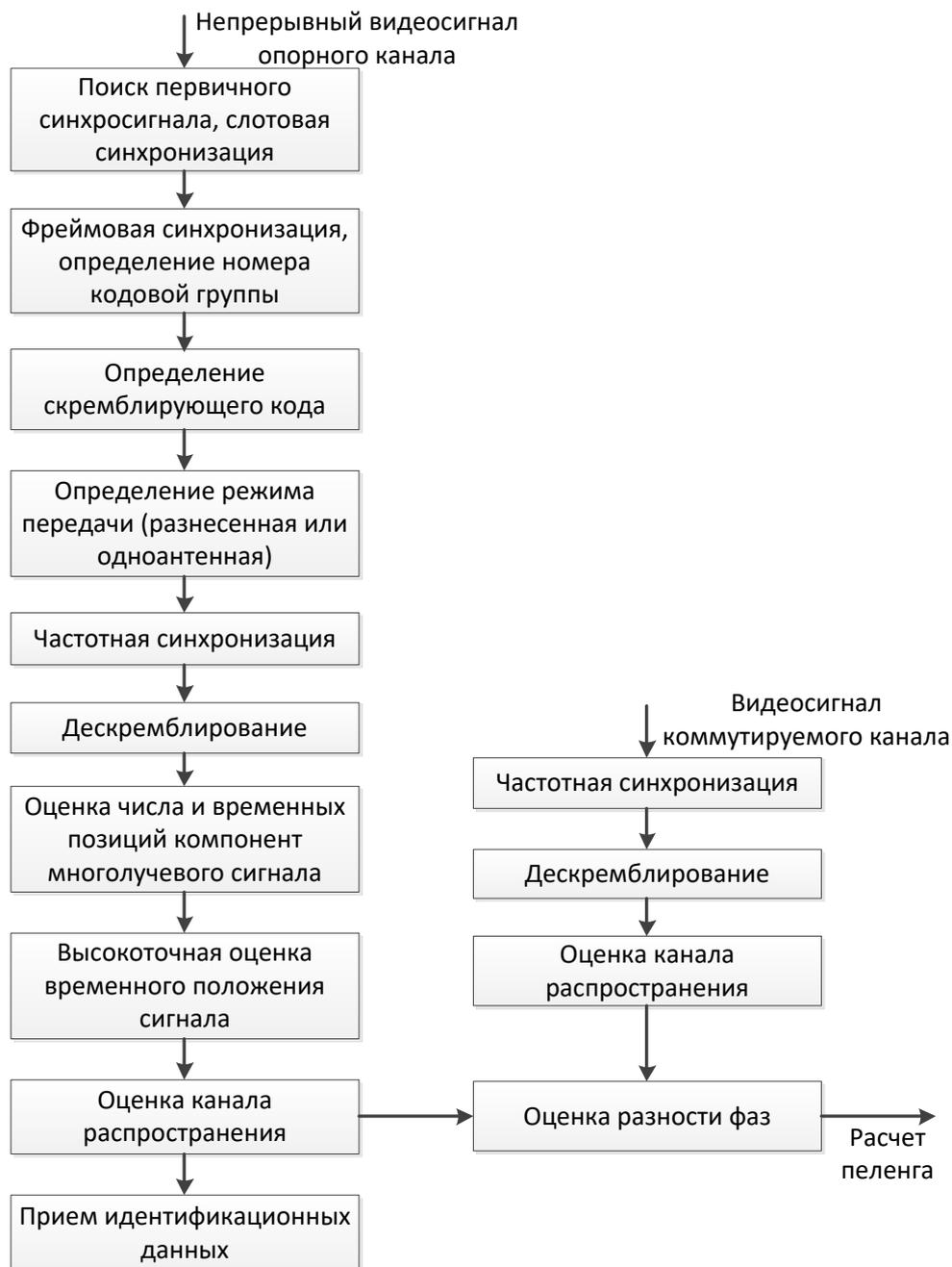


Рис. 2. Блок-схема пеленгования UMTS сигнала

Частотная синхронизация выполняется отдельно для каждой обнаруженной соты. Коррекция частоты для видеосигнала сигнального канала выполняется так же, как и для видеосигнала опорного канала

Дескремблирование видеосигнала сигнального канала для каждой обнаруженной соты осуществляется только для сигнала максимального первого по времени обнаруженного луча.

Далее формируется оценка канала для видеосигнала сигнального канала. Оценка канала выполняется для максимального сигнала первого по времени

луча каждой найденной соты последовательно для интервалов длиной  $L = 512$  чипов посредством накопления отсчетов на соответствующих интервалах. В одном фрейме имеется 75 интервалов длиной 512 чипов.

Соответствующие значения оценки канала при одноантенной и при двухантенной передаче получены для опорного канала в анализаторе.

Процедуры дескремблирования и оценки канала (накопление) обеспечивают подавление сигналов других сот как для сигнального, так и для опорного каналов.

Оценка канального комплексного коэффициента сигнального блока  $m$ -го элемента AP определяется, как сумма оценок канала интервалов слотов, целиком попадающих в интервал блока, как показано на рис. 3. Начальный отсчет блока  $m$ -го элемента AP попадает в некоторый интервал. Следующие за ним три интервала участвуют в получении комплексного коэффициента блока. Конечный отсчет блока попадает в четвертый интервал (так выбрана длина блока). Поскольку слотовая и фреймовая синхронизация установлена, начальный отсчет каждого из 75 интервалов фрейма известен. Выбор размера блока отсчетов для каждого элемента AP обусловлен квазистационарностью канала распространения на временном интервале блока.

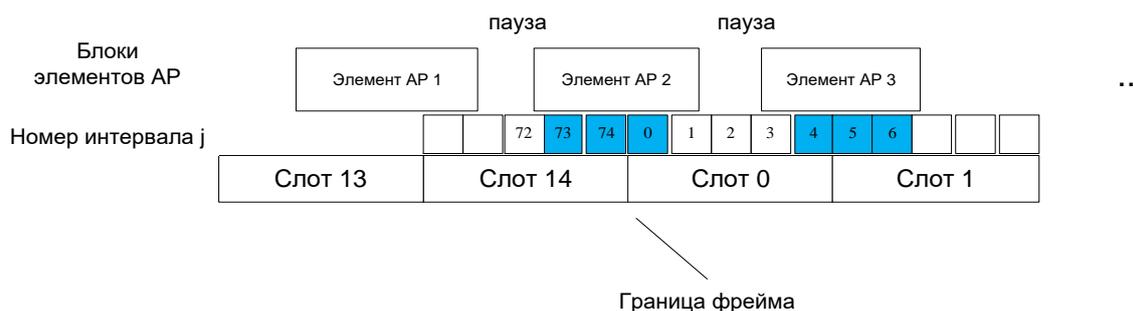


Рис. 3. Временная диаграмма пеленгования UMTS сигнала

При одноантенной передаче оценки канальных комплексных коэффициентов  $m$ -го  $B^{(m)}$  и нулевого  $B^{(0)}$  элементов AP равны сумме оценок канала трех соответствующих интервалов.

Оценка разности фаз между сигналами блоков  $m$ -го и нулевого элементов AP рассчитывается как

$$U_m = B^{(m)*} B^{(0)}, \quad m = \overline{0, M-1}. \quad (4)$$

При двухантенной передаче оценка разности фаз между сигналами блоков  $m$ -го и нулевого элементов AP равна

$$U_m = B1^{(m)} B1^{(0)*} + B2^{(m)} B2^{(0)*}, \quad m = \overline{0, M-1}. \quad (5)$$

где  $B1^{(m)}$ ,  $B1^{(0)}$  – оценка канальных комплексных коэффициентов  $m$ -го и нулевого элементов AP для первой передающей антенны,  $B2^{(m)}$ ,  $B2^{(0)}$  – оценка канальных комплексных коэффициентов  $m$ -го и нулевого элементов AP для второй передающей антенны.

### Пеленгование БС LTE

Для LTE систем в прямом канале используется технология OFDMA (Orthogonal Frequency Division Multiple Access) [3]. При этом сигналы различных сот сети передаются одновременно в одном спектральном диапазоне. Ширина полосы сигнала LTE может принимать одно из следующих значений: 1,4; 3; 5; 10; 15; 20 МГц. Каждая сота характеризуется идентификаторами физического и системного уровней.

Сигнал LTE соты включает совокупность различных физических каналов, передаваемых в определенных местах частотно-временной области сигнала. Для обнаружения соты и получения ее идентификатора физического уровня достаточно приема первичного и вторичного синхросигналов, а также широковещательного канала, передаваемых в полосе 1,4 МГц. Для получения идентификаторов системного уровня необходим также прием других каналов: канала гибридной ARQ (Automatic Repeat Request), канала индикатора контрольного канала, контрольного канала и совместного канала. Эти каналы передаются в полной полосе LTE сигнала.

Соответствие между идентификатором физического уровня и идентификаторами системного уровня устанавливает анализатор, хотя бы один раз обнаруживший ту или иную соту.

Для пеленгования обнаруженных сот достаточно работать с полосой 1.4 МГц, в которой передается идентификатор физического уровня этих сот. Последовательность обработки сигнала LTE при пеленговании показана на рис. 4.



Рис. 4. Блок-схема пеленгования LTE сигнала

Исходными данными для пеленгования являются два комплексных видеосигнала  $x_{0i}$ ,  $x_{1i}^{(m)}$ ,  $i = 0, 1, \dots, N - 1$  с частотой дискретизации  $f_s = 1,92$  МГц, полоса сигнала 1,4 МГц. Непрерывный комплексный видеосигнал опорного канала LTE обрабатывается в соответствии с процедурами, описанными в [3], и указанными на рис. 4. Среди этих процедур обнаружение базовых станций (сот), определение номера сектора БС физического уровня, частотно-временная синхронизация, определение длины префикса, фреймовая синхронизация, определение идентификатора соты физического уровня и режима дуплекса, прием сообщения широкополосного канала.

Оценка разности фаз сигнала базовых станций LTE производится с учетом хороших корреляционных свойств первичного синхросигнала, который представляет собой комплексные элементы последовательности Zadoff-Chu с одним из трех значений параметра, определяемым сектором базовой станции. Для LTE систем с частотным разделением (FDD) он передается в последних OFDM символах слотов 0 и 10, для систем с временным разделением – в третьих OFDM символах сабфреймов 1 и 6 каждого фрейма.

Длина блока отсчетов видеосигнала каждого элемента AP выбрана так, чтобы в каждом блоке гарантированно присутствовал OFDM символ с первичным синхросигналом (приблизительно 5 мс). После установления частотно-временной синхронизации временное положение символов первичного синхросигнала известно. Для опорного и сигнального каналов формируются величины

$$B_r^{(0)} = \sum_{n=0}^{255} x_{0,n+j+K \cdot r} \cdot P_n^*, \quad B_r^{(m)} = \sum_{n=0}^{255} x_{1,n+j+K \cdot r}^{(m)} \cdot P_n^* \quad (6)$$

где  $K$  – период повторения символов первичного синхросигнала,  $j$  – отсчет начала первичного синхросигнала (результат начальной синхронизации),  $P_n$ ,  $n = \overline{0, 255}$  – известный опорный сигнал, представляющий собой результат обратного ДПФ длиной 256 от последовательности Zadoff-Chu с соответствующим параметром  $u$ , определенным в процедуре обнаружения ( $u = 25$  или  $u = 29$  или  $u = 34$ ).

В величинах (6) на выходе корреляторов сигналы других обнаруженных сот являются подавленными.

Окончательно оценка разности фаз между сигналами блоков  $m$ -го и опорного элементов AP равна

$$U_m = B_r^{(m)*} B_r^{(0)}, \quad m = \overline{0, M - 1}. \quad (7)$$

### Примеры адресного пеленгования

Приведем примеры работы комплекса идентификации и пеленгования сигналов БС GSM, UMTS, LTE сетей сотовой связи, реализованного на базе мобильного пеленгатора АРТИКУЛ-М. Этот пеленгатор включает антенную систему в радиопрозрачном обтекателе с двухканальным цифровым радиоприемным устройством и аппаратурой навигации. Функционал обнаружения, анализа и пеленгования обнаруженных БС реализован в виде программного моду-

ля, осуществляющего функцию обнаружения, анализа и пеленгования обнаруженных БС.

Примеры работы анализатора сигналов БС GSM, UMTS, LTE и их описание представлены в [1-3]. Для визуализации результатов пеленгования используется усредненная по циклам пеленгования решающая функция (желтым цветом), гистограмма пеленгов (красным цветом), по которой рассчитывается направление на БС.

Для всех сотовых систем GSM, UMTS и LTE процедура пеленгования является единообразной. В качестве примера на рис. 5 показаны результаты пеленгования сигнала БС GSM. Гистограмма на рис. 5 построена по 127 пеленгам.

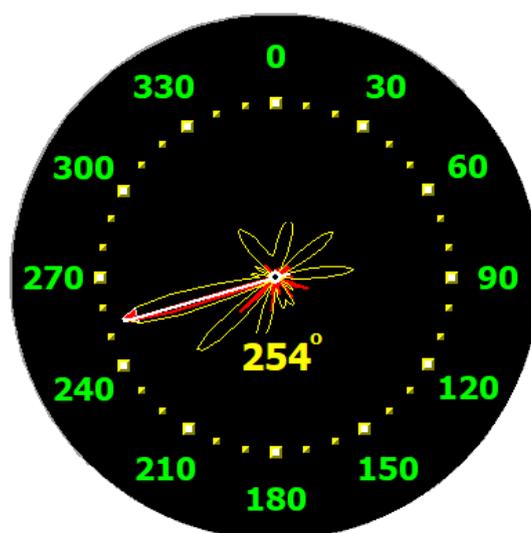


Рис. 5. Пример результатов пеленгования БС GSM

По результатам пеленгования в различных точках траектории мобильного пеленгатора можно получить оценку местоположения обнаруженных БС, например, с использованием угломерной или амплитудно-угломерной информации [4-6, 16]. На рис. 6 показан пример оценки местоположения БС GSM с номером 4043. На фоне карты местности цветом показана двумерная решающая функция оценки местоположения обнаруженной БС, а также положение точек местности, в которых получены результаты пеленгования. Красный цвет соответствует наибольшим значениям решающей функции. Реальное расположение базовой станции практически совпадает с полученной оценкой (черная точка).

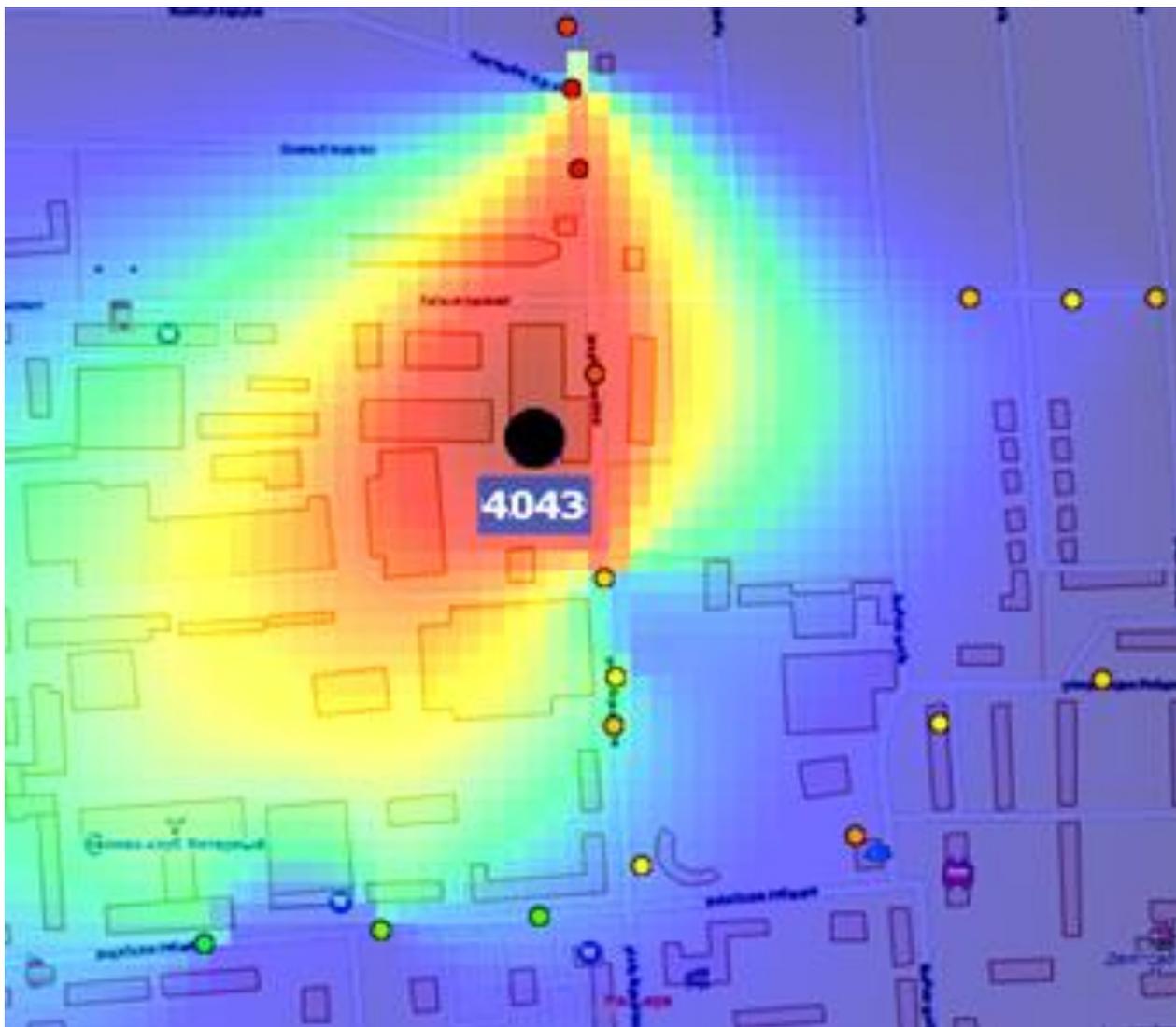
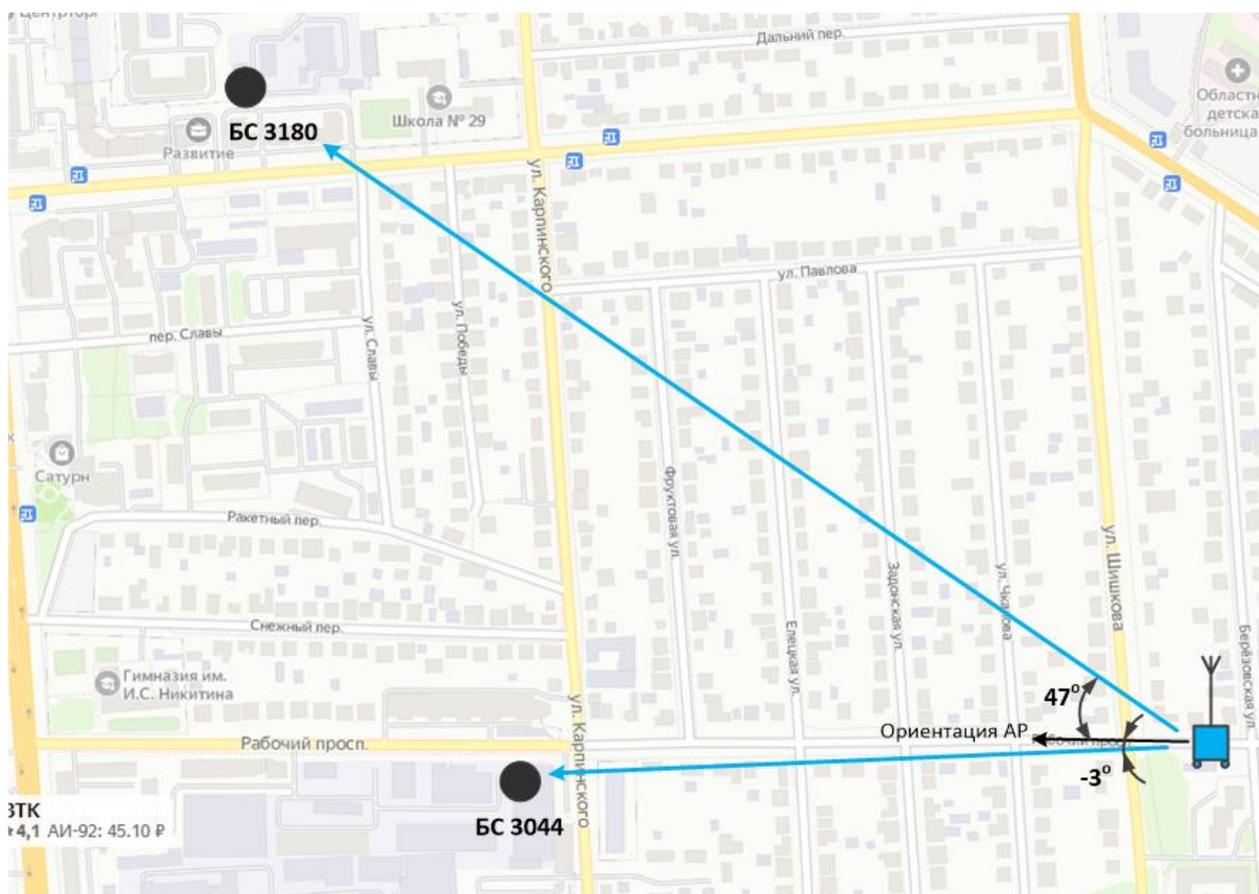
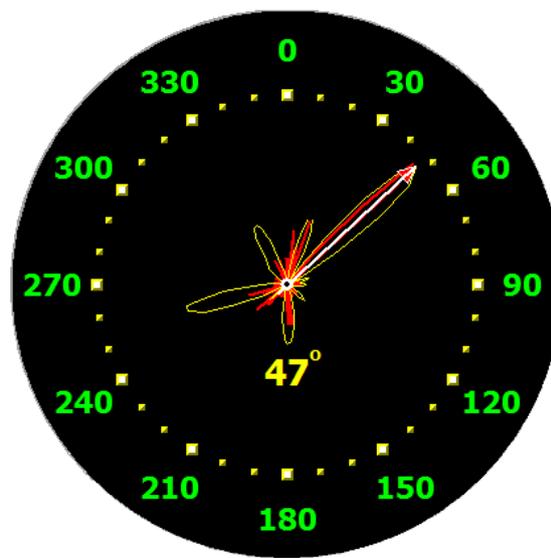


Рис. 6. Пример оценки местоположения БС GSM

В процессе пеленгования базовых станций UMTS и LTE в городских условиях часто возникает ситуация, когда в точке анализа обнаружены сигналы нескольких пространственно разнесенных БС. На рис. 7 представлен пример пеленгования двух базовых станций UMTS с номерами 3044 и 3180, расположенных на расстоянии приблизительно 800 м друг от друга. На карте рис. 7 показано реальное расположение пеленгуемых базовых станций UMTS, координаты пеленгатора и ориентация его антенной решетки (черной стрелкой), а также направления пеленгов на обнаруженные БС. Снизу на рис. 7 показаны полученные результаты пеленгования: усредненные решающие функции и гистограммы пеленгов.



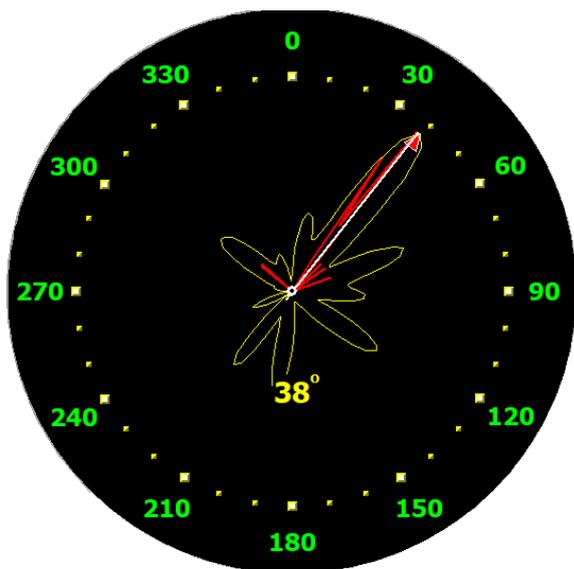
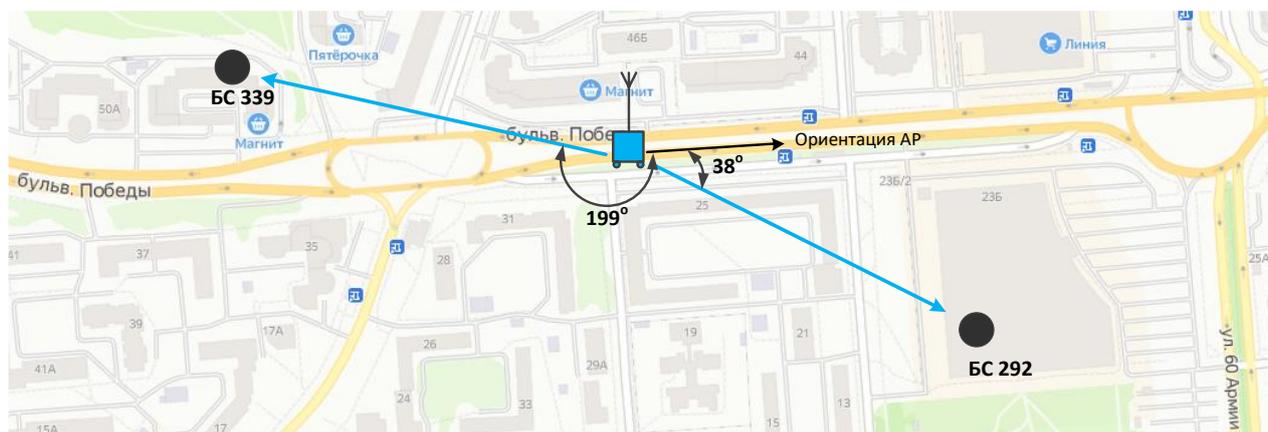
Результат пеленгования BC 3044



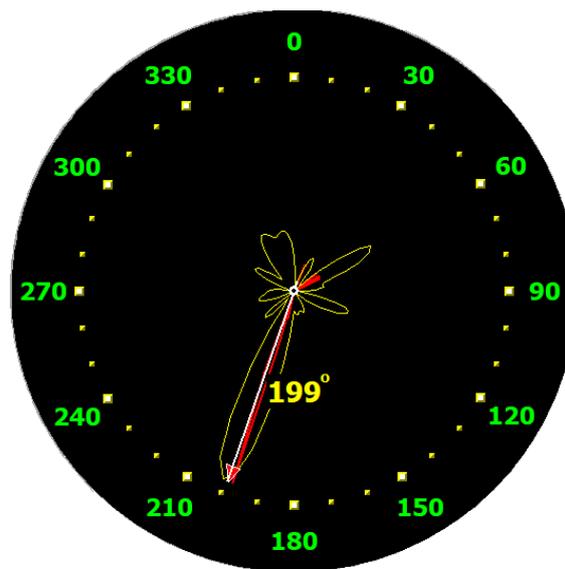
Результат пеленгования BC 3180

Рис. 7. Пример адресного пеленгования BC UMTS

На рис. 8 приведен аналогичный пример пеленгования двух обнаруженных BC LTE с номерами 339 и 292. Расстояние между базовыми станциями – 700 м, мобильный пеленгатор расположен между ними, уровни сигналов от BC в точке приема примерно равны. Результаты пеленгования соответствуют известным направлениям на BC, показанным на карте.



Результат пеленгования БС 292



Результат пеленгования БС 339

Рис. 8. Пример адресного пеленгования БС LTE

### Заключение

В данной статье разработан способ адресного пеленгования, использующий информацию о тонкой структуре сигналов БС систем GSM, UMTS, LTE. Он позволяет выполнить обнаружение и идентификацию всех обнаруженных БС и сформировать оценку направления на эти БС.

Разработанный способ пеленгования внедрен и успешно апробирован в аппаратно-программном комплексе пеленгования сигналов базовых станций на базе корреляционно-интерферометрического пеленгатора АРТИКУЛ-М.

Использование адресного пеленгования БС сотовых систем увеличивает функциональные возможности существующих анализаторов сотовых систем связи, позволяет определять местоположение базовых станций.

### Литература

1. Ашихмин А. В., Каюков И. В., Козьмин В. А., Манелис В. Б. Анализатор базовых станций GSM сетей на базе панорамного измерительного приемника АРГАМАК-ИМ // Специальная техника. 2008. № 1. С. 31-39.

2. Алексеев П. А., Ашихмин А. В., Каюков И. В., Козьмин В. А., Манелис В. Б. Анализатор сигналов базовых станций UMTS сетей // Спецтехника и связь. 2012. № 5-6. С. 57-68.
3. Алексеев П. А., Ашихмин А. В., Беспалов О. В., Каюков И. В., Козьмин В. А., Манелис В. Б. Анализатор сигналов базовых станций GSM, UMTS, LTE сетей сотовой связи // Спецтехника и связь. 2016. №4. С. 50-59.
4. Рембовский А. М., Ашихмин А. В., Козьмин В. А. Радиомониторинг – задачи, методы, средства / под ред. А.М. Рембовского. – М.: Горячая линия-Телеком, 2015. – 640 с.
5. Рембовский А. М., Ашихмин А. В., Козьмин В. А., Автоматизированные системы радиоконтроля и их компоненты / под ред. А. М. Рембовского. – М.: Горячая линия-Телеком, 2017. – 424 с.
6. Rembovsky A. M., Ashikhmin A. V., Kozmin V. A., Smolskiy S. M. Radio Monitoring Automated Systems and Their Components. – Springer, 2018. – 467 p.
7. Zekavat R., Buehrer R. M. Handbook of Position Location: Theory, Practice and Advances. – John Wiley & Sons, 2011. – Vol. 27.
8. Schmidt R. O. Multiple Emitter Location and Signal Parameter Estimation // IEEE Antennas and Propagation. 1986. Vol. AP-34. P. 276-280.
9. Abdalla M. M., Abuitbel M. B., Hassan M. A. Performance Evaluation of Direction of Arrival Estimation Using MUSIC and ESPRIT Algorithms for Mobile Communication Systems // 6th Joint IFIP Wireless and Mobile Networking Conference (WMNC). 2013. P. 1-7.
10. Chiang C. T., Chang A. C. DOA Estimation in the Asynchronous DS-CDMA System // IEEE Transactions on Antennas and Propagation. 2003. Vol. 51. P. 40-47.
11. Del Re E., Pierucci L., Marapodi S. On the application of DOA estimation techniques to UMTS system // IEEE Seventh International Symposium on Spread Spectrum Techniques and Applications. 2002. Vol. 2. P. 550-554.
12. Morrison A., Sharif B. S. High-resolution iterative DOA algorithm for W-CDMA space-time receiver structures // IEEE 54th Vehicular Technology Conference. 2001. Vol. 1. P. 380-384.
13. Ko Y.H., Park C.H., Cho Y.S. Joint Methods of Cell Searching and DoA Estimation for a Mobile Relay Station with Multiple Antennas // IEEE GLOBECOM. 2008. P. 1-4.
14. Pec R., Cho Y.S. A Parameter Estimation Technique for an LTE-based Mobile Relay Station with Antenna Array // 2013 International Conference on ICT Convergence (ICTC). 2013. P. 134-135.
15. Гельгор А. Л., Павленко И. И., Фокин Г. А., Горлов А. И., Попов Е. А., Лаврухин В. А., Сиверс М. А. Пеленгация базовых станций в сетях LTE // Электросвязь. 2014. № 9. С. 34-39.
16. Козьмин В. А., Савельев А. М., Уфаев В. А., Чубов Е. А. Сравнение методов местоопределения источников радиоизлучения // Специальная техника. 2007. № 1. С. 30-38.

## References

1. Ashikhmin A. V., Kayukov I. V., Kozmin V. A., Manelis V. B. Analizator bazovykh stantsiy GSM setey na baze panoramnogo izmeritel'nogo priyemnika ARGAMAK-IM [Analyzer of base stations of GSM networks based on panoramic measuring receiver ARGAMAK-IM]. *Spetsial'naiia Tekhnika*, 2008, no. 1, pp. 31-39 (in Russian).
2. Alexeev P. A., Ashikhmin A. V., Kayukov I. V., Kozmin V. A., Manelis V. B. Analizator signalov bazovykh stantsiy UMTS setey [Signal analyzer of base stations of UMTS networks]. *Specialized Machinery and Communication*, 2012, no. 5-6, pp. 57-68 (in Russian).
3. Alexeev P. A., Ashikhmin A. V., Bepalov O. V., Kayukov I. V., Kozmin V. A., Manelis V. B. Analizator signalov bazovykh stantsiy GSM, UMTS, LTE setey sotovoy svyazi [Signal analyzer of base stations GSM, UMTS, LTE cellular networks]. *Specialized Machinery and Communication*, 2016, no. 4, pp. 50-59 (in Russian).
4. Rembovsky A. M., Ashikhmin A. V., Kozmin V. A. *Radiomonitoring – zadachi, metody, sredstva* [Radio monitoring – tasks, methods, means]. Moscow, Hotline-Telecom, 2015. 640 p. (in Russian).
5. Rembovsky A. M., Ashikhmin A. V., Kozmin V. A. *Avtomatizirovannyye sistemy radiokontrolya i ikh komponenty* [Automated radio monitoring systems and their components]. Moscow, Hotline-Telecom, 2017. 424 p. (in Russian).
6. Rembovsky A. M., Ashikhmin A. V., Kozmin V. A., Smolskiy S. M. *Radio Monitoring Automated Systems and Their Components*. Springer, 2018. 467 p.
7. Zekavat R., Buehrer R. M. *Handbook of Position Location: Theory, Practice and Advances*. Natick, John Wiley & Sons, 2011. Vol. 27.
8. Schmidt R. O. Multiple Emitter Location and Signal Parameter Estimation. *IEEE Antennas and Propagation*, 1986, vol. AP-34, pp. 276-280.
9. Abdalla M. M., Abuitbel M. B., Hassan M. A. Performance Evaluation of Direction of Arrival Estimation Using MUSIC and ESPRIT Algorithms for Mobile Communication Systems. *6th Joint IFIP Wireless and Mobile Networking Conference (WMNC)*, 2013, pp. 1-7.
10. Chiang C. T., Chang A. C. DOA Estimation in the Asynchronous DS-CDMA System. *IEEE Transactions on Antennas and Propagation*, 2003, vol. 51, pp. 40-47.
11. Del Re E., Pierucci L., Marapodi S. On the application of DOA estimation techniques to UMTS system. *IEEE Seventh International Symposium on Spread Spectrum Techniques and Applications*, 2002, vol. 2, pp. 550-554.
12. Morrison A., Sharif B. S. High-resolution iterative DOA algorithm for W-CDMA space-time receiver structures. *IEEE 54th Vehicular Technology Conference*, 2001, vol. 1, pp. 380-384.
13. Ko Y. H., Park C. H., Cho Y. S. Joint Methods of Cell Searching and DoA Estimation for a Mobile Relay Station with Multiple Antennas. *IEEE GLOBECOM*, 2008, pp. 1-4.

14. Pec R., Cho Y.S. A Parameter Estimation Technique for an LTE-based Mobile Relay Station with Antenna Array. *2013 International Conference on ICT Convergence (ICTC)*, 2013, pp. 134-135.

15. Gelgor A. L., Pavlenko I. I., Fokin G. A., Gorlov A. I., Popov E. A., Lavrukhin V. A., Sivers M. A. Direction finding of base stations in LTE networks. *Electrosvyaz*, 2014, no 9, pp. 34-39 (in Russian).

16. Kozmin V. A., Savelyev A. M., Ufaev V. A., Chubov E. A. Sravneniye metodov mestoopredeleniya istochnikov radioizlucheniya [Comparison of methods for radio sources localization]. *Spetsial'naiia Tekhnika*, 2007, no 1, pp. 30-38 (in Russian).

Статья поступила 29 марта 2021 г.

### Информация об авторах

*Манелис Владимир Борисович* – доктор технических наук. Ведущий научный сотрудник. АО «ИРКОС». Область научных интересов: системы связи, радиомониторинг, алгоритмы приема и обработки сигналов. E-mail: vldman@mail.ru

*Сладких Владимир Александрович* – кандидат технических наук. Начальник научно-исследовательского сектора. АО «ИРКОС». Область научных интересов: радиомониторинг, цифровая обработка сигналов. E-mail: sladkihv@mail.ru.

*Козьмин Владимир Алексеевич* – кандидат технических наук, доцент. Директор по научной работе. АО «ИРКОС». Область научных интересов: радиомониторинг, цифровая обработка сигналов. E-mail: kozminva@ircos.vrn.ru

*Бизюков Павел Евгеньевич* – аспирант. Инженер по обеспечению качества программного обеспечения. АО «ИРКОС». Область научных интересов: радиомониторинг, цифровая обработка сигналов. E-mail: bizukovpe@ircos.vrn.ru.

Адрес: 394024, Россия, г. Воронеж, Рабочий пр., д. 101б.

---

## Base station address direction finding of GSM, UMTS, LTE cellular networks

V. B. Manelis, V. A. Sladkikh, V. A. Kozmin, P.E. Bizyukov

**Problem statement:** Cellular networks of European digital standards GSM, UMTS, LTE are very popular in Russia and other countries. The need to identify unauthorized base stations (BS) of these networks, check compliance with the frequency-territorial plan, check the deviation of the BS location from the conditions of the issued permits requires operators and radio monitoring services to analyze BS signals, including their direction finding and position estimation. Many BS of cellular networks, characterized by their identification parameters, carry out simultaneous transmission in the same frequency range and interfere with each other. This makes it impossible to use phase-difference direction finding methods and requires the development of new methods for joint identification, direction finding and position estimation of BS. **The aim of the work** is to develop algorithms for joint identification and direction finding of detected base stations of GSM, UMTS, LTE cellular networks. **Novelty:** a method of radio monitoring is presented, which implements the function of address direction finding of base stations of GSM, UMTS, LTE networks. In this case, accord-

ing to the received signal implementation, simultaneous identification and direction finding of all detected BSs is carried out. The implementation of the presented method is based on the use of BS analyzers of these networks, includes a two-channel radio receiver with navigation equipment and an antenna array. Analyzers implement "targeting", and a two-channel receiver and an antenna array - direction finding of detected BSs with reference to their identifiers. **Results:** the developed method for addressing direction finding, using information on the fine structure of BS signals, make it possible to detect and identify all detected BSs and form an estimate of the direction to these BSs. The developed method of direction finding was implemented and successfully tested in the hardware and software complex for direction finding signals from base stations based on the ARTIKUL-M direction finder. **Practical relevance:** the use of addressable direction finding of BS of cellular systems increases the functionality of existing analyzers of cellular communication systems and makes it possible to determine the location of base stations.

**Keywords:** GSM, UMTS, LTE, base station, signal analyzer, identification parameters, direction finding.

### Information about Authors

*Vladimir Borisovich Manelis* – holder of an Advanced Doctorate in Engineering Sciences. Leading Researcher. JSC «IRCOS». Field of research: communication systems, radiomonitoring, algorithms for receiving and processing signals. E-mail: vldman@mail.ru

*Vladimir Alexandrovich Sladkikh* – Ph.D. of Engineering Sciences. Head of the Research Sector. JSC «IRCOS». Field of research: radiomonitoring, digital signal processing. E-mail: sladkih@mail.ru.

*Vladimir Alexeevich Kozmin* – Ph.D. of Engineering Sciences, Associate Professor. Director for Scientific Work. JSC «IRCOS». Field of research: radiomonitoring, digital signal processing. E-mail: kozminva@ircoc.vrn.ru

*Pavel Evgenievich Bizyukov* – Postgraduate Student. Software Quality Assurance Engineer. JSC «IRCOS». Field of research: radiomonitoring, digital signal processing. E-mail: bizukovpe@ircoc.vrn.ru

Address: 394024, Russia, Voronezh, Rabochiy prospect, 101b.