УДК 621.382

БЛОКИРОВАНИЕ ТЕРМИНАЛОВ СОТОВОЙ СВЯЗИ

А.Г. ГАЛКИН, В.К. КОНОПЕЛЬКО

Белорусский государственный университет информатики и радиоэлектроники
П. Бровки, 6, Минск, 220013, Беларусь

Поступила в редакцию 30 января 2007

В статье приведен анализ используемых методов блокирования терминалов сотовой связи. Показано, что системное блокирование обеспечивает гарантированное закрытие и выполнение всех требований по контролю за необходимыми соединениями в зоне закрытия.

Ключевые слова: блокиратор сотовой связи, джамминг, "глушитель", интеллектуальный блокиратор, системный блокиратор.

Постановка задачи

Интенсивное развитие сетей мобильной связи делает актуальной проблему организации зон гарантированного радиомолчания на режимных объектах во время проведения специальных мероприятий, в том числе при необходимости обеспечения быстрого реагирования и развертывания системного блокиратора. В связи с этим возникает задача выполнения следующих основных требований.

1. Оперативная организация зон, в которых было бы гарантированно невозможно воспользоваться терминалами сотовой связи.

2. Реализация обеспечения без использования постоянного генератора электромагнитных помех, негативно воздействующих на людей и высокоточную технику (медицинские учреждения, научно-технические центры).

3. Возможность организации таких зон в любых населенных пунктах, вне населенных пунктов, как в зданиях и сооружениях, так и на открытых площадках.

4. Отсутствие зависимости от сетевой инфраструктуры, функциональных особенностей сетей сотовой связи осуществляющих покрытие в зоне блокирования, типа терминала, его производителя.

5. Скрытность воздействия.

Наряду с основными требованиями практическое использование существующих блокираторов привело к появлению дополнительных задач, выполнение которых не носит обязательного характера (ввиду сложности (невозможности) реализации существующими устройствами), однако в реальных условиях почти всегда необходимо. Это следующие задачи:

1) реализация возможности организации VIP-списков абонентов, которым сохраняется возможность беспрепятственного общения внутри обеспечиваемой зоны;

2) возможность частичного закрытия выбранных абонентов, находящихся внутри зоны с обеспечением полного контроля за разрешенными к установлению соединениями;

3) фиксация любой сетевой активности и всех разрешенных соединений выбранных абонентов.

Оценка реализованных решений

Блокираторы сотовых телефонов можно подразделить в зависимости от способа блокировки на два типа: с использованием различных методов воздействия на электромагнитные волны и применением опциональных возможностей сетей и аппаратов сотовой связи [1]. Рассмотрим эффективность применения реализованных решений для выполнения условий поставленной задачи[2].

Экранирующие панели. Достоинством этого метода является то, что подобные устройства являются практически единственной альтернативой активных блокираторов. Их применение целесообразно в местах, где недопустимо любое излучение (аппаратные с высокочувствительными приборами, высокоточные измерительные комплексы и т.п.), либо законодательно определено отсутствие альтернативы. Недостатки же определяются тем, что устройства работают только в закрытых помещениях, из-за необходимости экранирования по всему объему. Кроме этого производители гарантируют эффективность не выше 97%.

Устройства, взаимодействующие с сетью. Устройства данного типа позволяют производить блокировку сотовых терминалов, используя только оговоренные сигнальные каналы. При полной реализации возможна высокая эффективность в сочетании с относительно низкими затратами, что является достоинством этих приборов. Недостатки определяются тем, что подобная опциональная функция сети практически нигде не реализована. Помимо этого, для действенного применения необходимо предоставление названной услуги всеми операторами сотовой связи, осуществляющими покрытие данного региона. Необходимо также помнить, что, поскольку эта функция будет носить глобальный характер, для не специального использования нужно обеспечить VIP-списки терминалов, которые нельзя блокировать ни при каких условиях. Следствием чего будет негарантированная эффективность. Отличительной чертой подобных устройств является обязательная привязка к реальным условиям эксплуатации.

Устройства, взаимодействующие с терминалами сотовой связи. Особенностью этих устройств является то, что они позволяют избежать возможности инициализации вызова (имеется в виду полное отсутствие сигнального обмена, связанного с установлением соединения). Это обусловлено тем, что прибор взаимодействует непосредственно с абонентским терминалом и в ходе диалога переводит его в режим радиомолчания. Однако на сегодняшний день меньшая часть использующихся аппаратов сотовой связи оборудована необходимыми интерфейсами (Bluetooth, IR-порт). Кроме того, при взаимодействии с IR-портом необходимо реализовать режим прямой видимости, что в условиях реальной эксплуатации терминалов практически не выполнимо. В реальных условиях применение подобных устройств малоэффективно.

Физический досмотр с применением спецсредств. Этот способ в случае возможности тотального контроля, высокопрофессионального исполнения и использования металлодетекторов и устройств спецобнаружения позволяет добиться максимальной эффективности в блокировании не только сотовых терминалов, но и всех возможных несанкционированных средств связи. Наиболее существенными недостатками этого подхода являются: сложность его реализации при большом скоплении людей, отсутствие скрытности воздействия, невозможность контроля VIP-персон, человеческий фактор, возможный конфликт с правами человека, и высокая стоимость в случае необходимости обеспечения 100%-ного эффекта. Как показывает практика, возможно устранение некоторых из вышепреведенных недостатков. Для этого необходим подготовленный высококвалифицированный персонал, наличие спецоборудования в нужном объеме, возможность заблаговременного осмотра и подготовки объекта обеспечения, слаженная команда исполнителей, а также неукоснительное соблюдение всеми участниками процесса обеспечения, правил и норм проведения контроля. Данные требования, ввиду неадекватной затратности, в обычных условиях трудно выполнимы.

Активные генераторы помех. Основным достоинством подобных приборов является относительно низкая стоимость, в сочетании с условно высокой надежностью (что обусловлено правильностью выбора диапазона, в котором генерируется помеха, и мощностью излучаемого сигнала). Так же выделяется высокая степень мобильности, возможность быстрого развертывания и закрытия площадных зон необходимого радиуса. Очевидно, что при этом наблюдается постоянная активность источника при высоком уровне мощности. Это приводит к тому, что создаются помехи другим рядом расположенным электронным устройствам, а также возникает

возможность причинения вреда здоровью в случае активации вблизи человеческого тела. Так как функционирование подобных источников в обязательном порядке регулируется законодательством, возникает необходимость согласования с органами контроля за использованием РЧС и получения соответствующих разрешений в ведомствах, чьи интересы могут быть затронуты при использовании аппарата.

Согласно [3], активные генераторы помех сотовой связи делятся на три группы.

1. Блокираторы, представляющие собой генераторы помех с ручным управлением (WAC 1300E, Y3000), обеспечивающие постановку заградительной помехи в диапазоне частот работы базовых станций соответствующего стандарта.

2. Блокираторы, которые в своем составе кроме передатчика помех имеют еще и специальный приемник (Hammer, C-Guard-400 [4]), обеспечивающий прием сигналов в диапазонах частот работы передатчиков телефонных аппаратов соответствующего стандарта.

3. Интеллектуальные блокираторы (RS Multijamer [5]). Сравнительные характеристики активных и интеллектуальных генераторов помех приведены в таблице.

Сравнительные характеристики активных и интеллектуальных генераторов помех

Тип прибора	Модель	Производитель	Цена, евро	Блокируемые стандарты	Радиус обеспечения, м	Излучаемая мощность, Вт	Питание	Масса	Габариты
Активные генераторы помех	WAC 1300E	*Global Gadget Ltd.*, Великобритания	184	GSM 900/1800	15	0,2	– 9 В	85 г	122×56×25 мм
Активный блокиратор сотовых телефонов	C-Guard 400	*"РЭЙ-Защита информации"*, Россия	415	GSM 900/1800, CDMA	5	1	~ 9 В – 12 В 500 мА	350 г	245×85×98 мм
Генератор шума для блокировки несанкционированного включения мобильных телефонов (стационарный)	БСТ-JA	*"Спецтехника"*, Украина	495	GSM 900/1800, DAMPS, AMPS, CDMA	5–7	0,5	~ 220 В	Нет данных	Нет данных
Система обнаружения включения сотовых телефонов и их блокировки	Hammer Система состоит из трех отдельных приборов: сенсора, модуля подавления и пульта дистанционного управления	*"Конфидента"*, Россия	1780	GSM 900/1800. Опционально: AMPS, DAMPS, CDMA.	7	0,5	2×1,5 В типа AA / сетевой адаптер	500 г (без адаптера)	2×(195×115×45) мм
Сверхмощный блокиратор	Y3000	*Global Gadget Ltd.*, Великобритания	10500	Nextel, TDMA, CDMA, AMPS, NMTP, Etacs, GSM 900/1800, DCS, W-CDMA, PCS, 3G (UMTS, CDMA2000)	≥3000	Суммарная мощность 90	~ 110 В ~ 220 В или – 24 В/ 10 А	Блокир-р — 8 кг, антенна — 1,2 кг	Блокиратор: 435×315×225 мм Антенна: 340×185×83 мм
Универсальная аппаратура интеллектуального блокирования сотовой связи любых действующих стандартов внутри заданной зоны	RS multijam-mer Время обнаружения не более 200 мкс. При блокировании аппарата стандарта GSM суммарное время блокирования равно 4,8 мс	*"Радиосервис"*, Россия	45 000	NMT450i, AMPS/DAMPS, GSM900/1800, CDMA, DECT	до 50	3–4	~ 220 В	Нет данных	480×400×120 см (без антенн и компьютера управления)

Системное блокирование мобильных терминалов

Сотовые сети спроектированы таким образом, чтобы не допустить возможности несанкционированного доступа к ним со стороны мобильных терминалов (МТ), и в то же время возможность имитации базовой станции (БС) не ограничена [6].

Используя эти особенности, можно осуществить системное блокирование мобильных терминалов, реализовав следующие правила обработки:

1. На территории, где покрытие обеспечивают несколько операторов сотовой связи различных стандартов, определяется периметр, в котором необходимо обеспечить режим подавления (рис. 1).

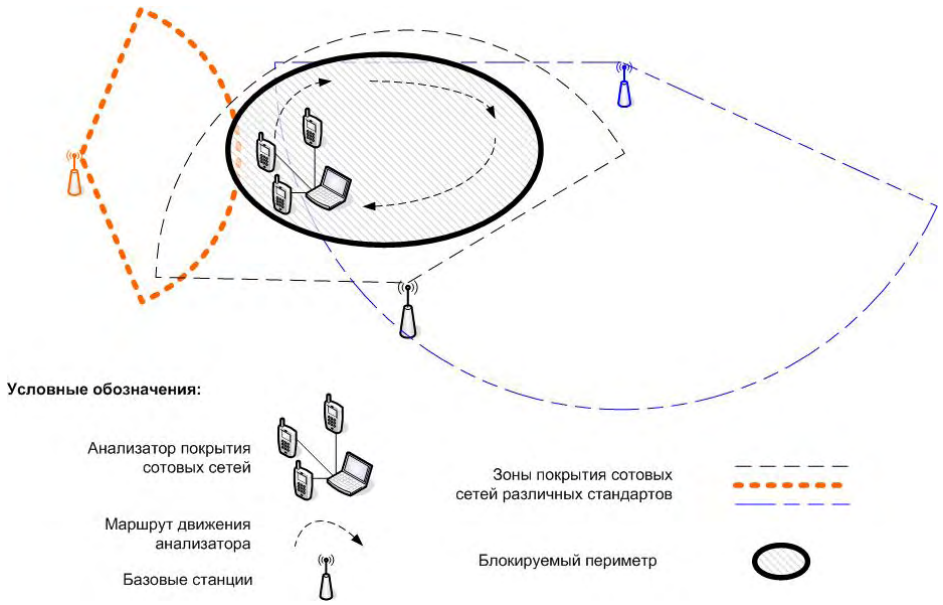


Рис. 1. Сбор исходных данных по покрытию в блокируемом периметре

2. Анализатор сканирует все диапазоны частот обеспечиваемого стандарта (GSM) и определяет те частоты, уровни которых в охраняемой области выше пороговых (рис. 2) (т.е. происходит имитация действий телефонных аппаратов для выявления тех частот, которые могут использоваться для мониторинга (рис. 2,*а*)). Одновременно совершается анализ и фиксация максимального уровня сигнала несущей (обычно это десятки пиковатт).

3. Выбираются частоты с уровнем, превышающим пороговый, для каждого диапазона каждого оператора. На выбранных частотах генерируется свой модулированный сигнальный канал (рис. 2,*б* "f1м"), с уровнем больше основного на отношение сигнал/шум для выбранного стандарта (для GSM это 9 дБ).

4. Одновременно устройство начинает генерировать по 1-й несущей (неиспользуемой в данном месте операторами) на стандарт для каждого оператора (например, если есть три GSM оператора которые работают как в DCS так и GSM диапазонах соответственно, необходимо генерировать шесть частот), с параметрами, однозначно интерпретируемыми аппаратами, находящимися в защищаемой зоне, как наилучшие (рис. 2,*б* "fн3d").

5. В созданных условиях терминалы производят перевыбор сигнальной частоты, и в отсутствие альтернативы выбирают для мониторинга псевдонесущую, излучаемую блокиратором, список соседних частот на которой выдается пустым (рис. 2,*в*).

Для аппаратной реализации необходим многочастотный модулятор, работающий во всех диапазонах используемых стандартов, широкополосные приемопередающие антенны. В качестве приемников-анализаторов могут выступать аппараты соответствующих стандартов. Все это необходимо подключить к ПЭВМ с программным обеспечением, позволяющим имитировать работу базовой станции.

Для обеспечения решения дополнительных задач необходимо дополнить устройство приемопередатчиками для взаимодействия с сетью. Так, например, для проверки VIP-списков схема взаимодействия, показанная на рис. 2, будет дополнена процедурой анализа номера (рис. 3). В случае если номер в VIP-списке не найден, ретрансляция не производится (рис. 3,*а*), иначе включается ретрансляция соединения (рис. 3,*б*).

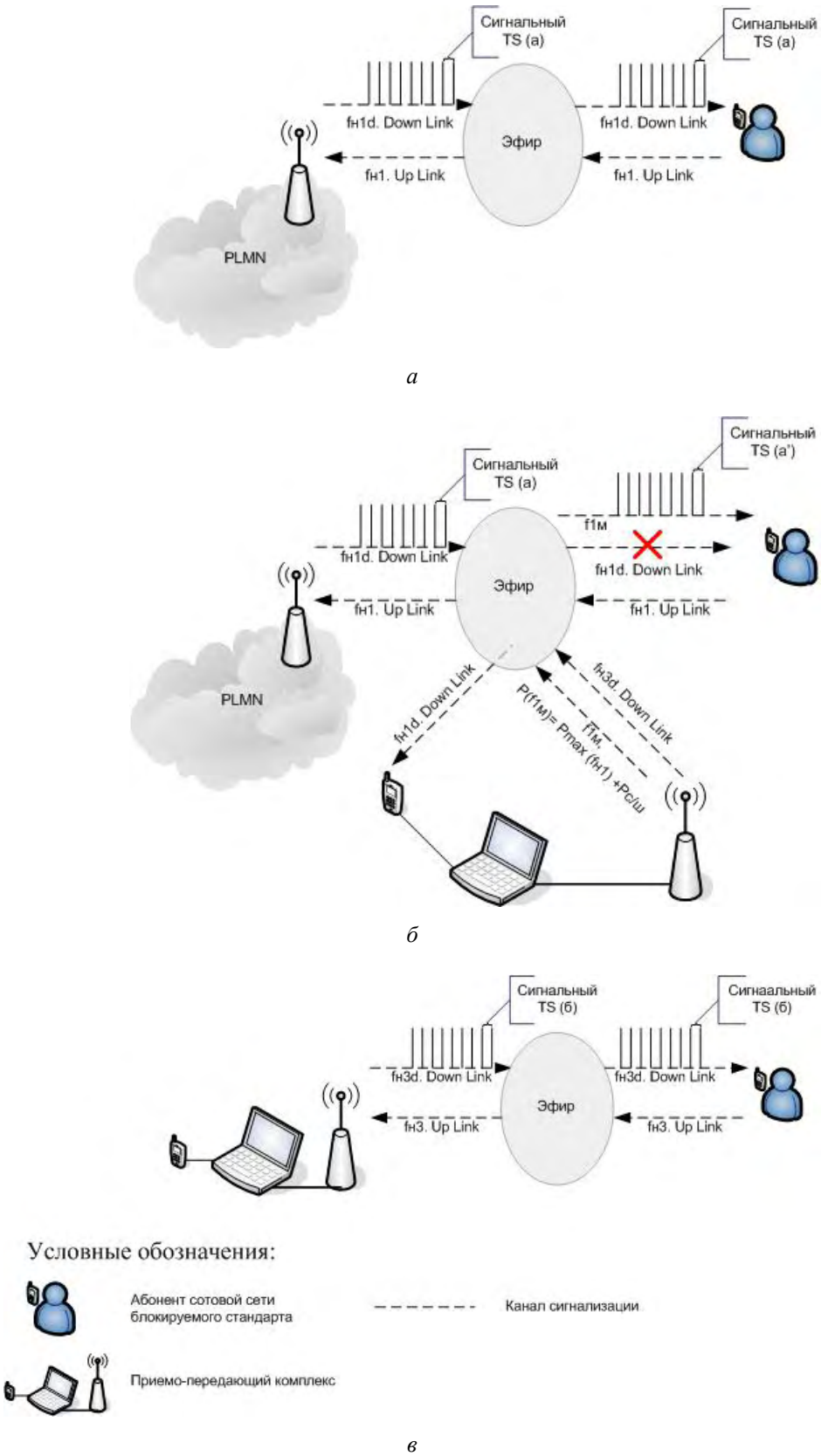
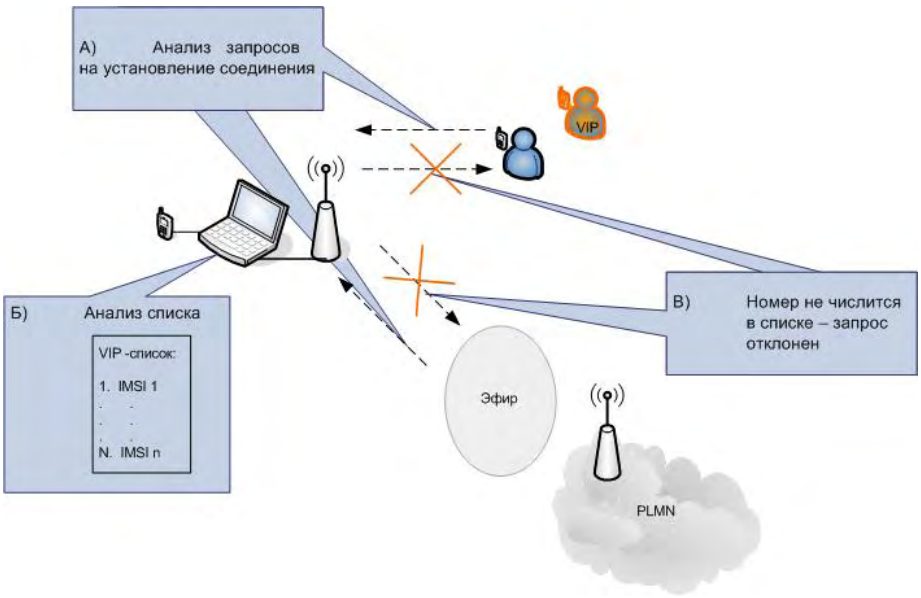
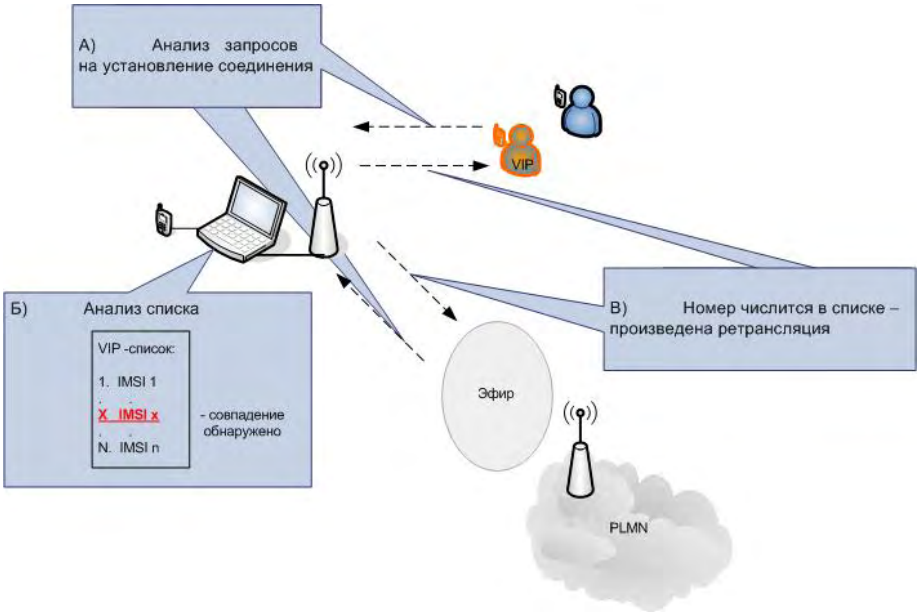


Рис. 2. Принцип работы системного блокиратора



а



б

Рис. 3. Сигнальное взаимодействие для обеспечения системных требований

Выводы

Использующиеся блокираторы аппаратов сотовой связи позволяют заблокировать в требуемом объеме терминалы практически всех используемых стандартов, однако не обеспечить блокировку относительно большой территории (50–1000 м^2) в случае, когда интенсивность попыток установления соединения (в достаточной степени обеспеченных сетью) превысит возможный порог реакции системы (например, учреждения пенитенциарной системы). Также невозможно с помощью имеющихся блокираторов в реальных условиях гарантированно исключить установление соединения. Кроме того, не существует подходов, позволяющих контролировать только обеспечиваемый объем, без организации дополнительного взаимодействия с оператором сотовой связи.

Для обеспечения этих функций необходимо разрабатывать устройства, использующие особенности сигнального обмена в сотовых сетях различных стандартов — системные блокираторы. Для реализации системного блокирования необходимы: многочастотный модулятор, работающий во всех диапазонах используемых стандартов, широкополосные приемопередающие антенны, а также ПЭВМ, имитирующая работу базовой станции.

THE CELL JAMMING

A.G. GALKIN, V.K. KONOPELKO

Abstract

In the article the brief analysis of used methods of blocking from the point of view of provision of requirements on provision of blocking is brought. From the same position the estimation developed by authors system-jammer from which it is visible is given, that this method provides the guaranteed closing and performance of all requirements. Besides system-jammer provides an opportunity of the supervision of necessary junctions in an area of provision.

Литература

1. *Федорчук М.* // Mobile News. 2003. № 28.
2. *Галкин А.Г., Конопелько В.К.* // Докл. БГУИР. 2005. № 6. С. 56–61
3. *Хореев А.А.* // Специальная техника. 2006. № 5. С. 55–64.
4. Технические системы и средства защиты информации: Информационные материалы. М., 2006.
5. Системы интеллектуального блокирования сотовой связи: Каталог. М., 2006.
6. *Галкин А.Г.* // Современные средства связи: Материалы XI Междунар. науч.-техн. конф. // Изв. Белорус. инж. акад. 2005. № 2.