УЧРЕЖДЕНИЕ ОБРАЗОВАНИЯ «БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ»

УДК 621.382

Галкин

Андрей Георгиевич

УПРАВЛЕНИЕ ДОСТУПОМ В МОБИЛЬНЫХ СЕТЯХ НА ОСНОВЕ СИСТЕМНОГО БЛОКИРОВАНИЯ

Автореферат диссертации на соискание ученой степени
кандидата технических наук
по специальности 05.13.19 – Методы и системы защиты информации, информационная безопасность

Минск, 2009

Работа выполнена в учреждении образования «Белорусский государственный университет информатики и радиоэлектроники»

Научный руководитель: **Конопелько Валерий Константинович**, доктор технических наук, профессор, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», заведующий кафедрой «Сети и устройства телекоммуникаций»

Официальные оппоненты: **Гейстер Сергей Романович,** доктор технических наук, профессор, Государственное учреждение «НИИ Вооруженных Сил Республики Беларусь», главный научный сотрудник

Горшков Сергей Анатольевич, кандидат технических наук, доцент, учреждение образования «Военная академия Республики Беларусь», начальник кафедры «Радиолокация и приемо-передающие устройства»

Оппонирующая организация: «Академия управления при Президенте Республики Беларусь»

Защита состоится 4 июня 2009 года в 16:00 на заседании совета по защите диссертаций Д 02.15.06 при учреждении образования «Белорусский государственный университет информатики и радиоэлектроники» по адресу: 220013, г. Минск, ул. П. Бровки, 6, ауд. 232-1, e-mail: dissovet@bsuir.by, тел. 293-89-89.

С диссертацией можно ознакомиться в библиотеке учреждения образования «Белорусский государственный университет информатики и радиоэлектроники».

Автореферат разослан «30» апреля 2009 г.

КРАТКОЕ ВВЕДЕНИЕ

При обеспечении информационной безопасности возникает необходимость управления доступом терминалов к мобильным сетям. Существующие методы управления доступом, основанные на использовании электромагнитных генераторов для подавления сигнальных частот без учета системных функций мобильных сетей, приводят к наличию постоянного сигнала с уровнем, превышающим фоновый, отсутствию скрытности и невозможности точного определения контролируемой зоны. Эти недостатки можно исключить при использовании методов управления доступом на основе учета сигнальных возможностей мобильных сетей. Актуальность темы диссертации обусловлена необходимостью разработки методов и средств управления доступом в мобильных сетях, позволяющих реализовать скрытную и оперативную защиту от утечки информации за пределы контролируемой зоны без использования постоянной генерации сигналов подавления.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Связь работы с крупными научными программами, темами

Исследования проводились в рамках Государственной комплексной программы научных исследований «Национальная безопасность» (2006 г.-наст. вр., № г. р. 20066846), по НИР ГБЦ 06-3106 «Исследование особенностей и разработка алгоритмов функционирования и программно-технических средств для силовых ведомств с целью их использования в телекоммуникационных системах с общим и санкционированным доступом», а также в рамках научно-исследовательской госбюджетной темы ГБ 06-2033 «Разработка методов обработки, передачи и распределения мультимедийной информации». Тема диссертационной работы соответствует приоритетным направлениям фундаментальных и прикладных исследований Республики Беларусь в области информационной безопасности, создания современных системы защиты информации.

Цель и задачи исследования

Целью настоящей диссертационной работы является разработка методов, алгоритмов и устройств управления доступом в мобильных сетях на основе системного блокирования для защиты от утечки информации за пределы контролируемой зоны.

Для достижения поставленной цели в диссертации необходимо решить следующие задачи.

1. Разработать методы и алгоритмы системного управления доступом мобильных терминалов к сетям GSM.

2. Разработать методику определения размеров контролируемой зоны.

3. Разработать методику оценки временных затрат на обеспечение контроля в защищаемом периметре.

4. Произвести экспериментальные исследования макета управления доступом мобильных терминалов к сетям GSM на основе системного блокирования.

Объектами исследования настоящей работы являются методы и средства скрытного и оперативного управления доступом в мобильных сетях на основе системного блокирования. Выбор данных объектов исследования обусловлен актуальностью проблемы защиты информации от несанкционированной передачи из контролируемой зоны. Эффективным подходом к решению этой проблемы является применение методов и алгоритмов управления доступом мобильных терминалов в контролируемой зоне, обеспечивающих их перерегистрацию на фиктивную базовую станцию.

Положения, выносимые на защиту

1. Метод, алгоритм и устройство системного управления доступом мобильных терминалов к сетям GSM на основе трансляции псевдонесущей, позволяющие понизить уровень излучаемого сигнала на 83 дБм при радиусе контролируемой зоны до 15 м по сравнению с методами частотного подавления.

2. Метод системного управления доступом в мобильных сетях на основе их пространственной локализации, позволяющий осуществлять блокирование доступа терминалов к сетям без генерации сигналов подавления.

3. Методика определения времени первичного блокирования мобильных терминалов, основанная на анализе параметров средств управления, что позволяет сократить время генерации сигнала подавления до 5 мин при использовании одной псевдонесущей для блокирования 100 терминалов.

4. Методика определения мощности сигналов подавления, основанная на адаптации их уровней в зависимости от зарегистрированной максимальной мощности по каждой опорной частоте, что позволяет снизить не менее чем на 75 % мощность передатчика устройства управления доступом терминалов к сетям GSM для обеспечения контролируемой зоны до 50 м по сравнению с методами частотного подавления.

Личный вклад соискателя

Основные научные и практические результаты диссертационной работы, а также положения, выносимые на защиту, разработаны и получены лично автором.

В совместно опубликованных работах автору принадлежат: разработка методов пространственной локализации и трансляции псевдонесущей; разработка методик определения зон, формируемых при системном блокировании, мощности транслируемых сигналов в режиме первичного блокирования и определения времени первичного блокирования мобильных терминалов; разработка алгоритма блокирования мобильных терминалов на псевдонесущей; разработка экспериментального макета управления доступом мобильных терминалов к сетям GSM, определение и выбор состава оборудования для его реализации и проведение натурных испытаний. Соавтором основных публикаций является научный руководитель, д.т.н., профессор В.К. Конопелько, который осуществлял определение целей и постановку задач исследования, выбор методов исследований, принимал участие в планировании работ и обсуждении результатов. Расчеты зон формируемых при системном блокировании, анализ и обсуждение результатов производились совместно со старшим преподавателем В.А. Аксеновым.

Апробация результатов диссертации

Основные положения и результаты диссертационной работы докладывались и обсуждались на следующих конференциях и семинарах различного уровня: 11-ой МНТК «Современные средства связи» - Нарочь, 2006 г.; «Современные средства связи»: материалы IX МНТК «Известия Белорусской инженерной академии». – Минск, 2004; «Телекоммуникации: сети и технологии, алгебраическое кодирование и безопасность данных»: международный научно-технический семинар Минск, БГУИР, 2006, 2007 г.

Опубликованность результатов

По результатам исследований, представленных в диссертации, опубликовано 11 печатных работ, в том числе: 8 статей в научных журналах общим объемом 3,2 авторских листа; 2 доклада в сборниках и материалах конференций; 1 патент на полезную модель.

Структура и объем диссертации

Работа состоит из введения, общей характеристики работы, четырех глав, заключения, списка использованных источников и приложений.

В первой главе проведен анализ процессов блокирования в инфокоммуникациях, структуры мобильных сетей стандарта GSM и методик планирования зон радиопокрытия. Во второй главе предложены методы управления доступом в мобильных сетях на основе пространственной локализации и трансляции псевдонесущей, разработаны методика, алгоритм и определена вероятность системного блокирования мобильных терминалов. В третьей главе произведена оценка временных затрат на первичное блокирование мобильных терминалов; разработаны методики определения формируемых зон при системном блокировании и мощности транслируемых сигналов. В четвертой главе произведены экспериментальные исследования макета системного блокирования и анализ полученных результатов. Общий объем диссертационной работы составляет 118 страниц, из которых 80 страниц текста, 43 рисунка на 25 страницах, 10 таблиц на 7 страницах, список использованных источников из 95 наименований на 7 страницах, 11 собственных публикаций автора на 2 страницах и 5 приложений на 7 страницах.

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Во введении определены основные направления исследований, обоснована актуальность темы диссертации, показана необходимость разработки и исследования методов, алгоритмов и устройств управления доступом в мобильных сетях на основе системного блокирования для обеспечения информационной безопасности.

В первой главе проведен анализ блокирования в информационных, коммутируемых (PSTN) и мобильных (PLMN) сетях, анализ преднамеренных угроз блокирования, структуры мобильных сетей стандарта GSM (англ. Global System for Mobile Communications - глобальная система мобильной связи) и методик планирования зон радиопокрытия, приведено обоснование направлений исследования и общей концепции работы.

Показано, что блокирование рассмотренное для информационных и коммутируемых сетей присутствует и в мобильных сетях. Блокирование в инфокоммуникациях означает как отказ в обслуживании, так и закрытие доступа, в результате чего ограничивается доступ терминалов (абонентов) к сетевым ресурсам (коммутатору). Блокирование терминалов в мобильных сетях, как правило, осуществляется без учета системных функций сетей и

производится с помощью электромагнитных генераторов путем воздействия на каналы доступа к сети (радиоканалы) [3-А].

Определены недостатки такого блокирования мобильных терминалов: наличие постоянного сигнала подавления с уровнем, превышающим фоновый (средний, детектируемый терминалами уровень сигнала мобильных сетей), отсутствие скрытности, невозможность точного определения контролируемой зоны [1-А]. Установлена необходимость разработки методов управления доступом в мобильных сетях, позволяющих реализовать скрытное и оперативное блокирование заданной территории без постоянной (периодической) генерации сигналов подавления с уровнем, превышающим фоновый.

Проведен анализ принципов построения и особенностей планирования зон радиопокрытия мобильных сетей стандарта GSM [9-А]. Установлена возможность реализации устройства системного блокирования на основе имитации сетевого элемента (базовой станции) и использования для расчета контролируемой зоны применяемых на практике методик планирования зон радиопокрытия.

Во второй главе предложены методы управления доступом в мобильных сетях на основе пространственной локализации терминалов (МПЛ) и на основе трансляции псевдонесущей (МТП).

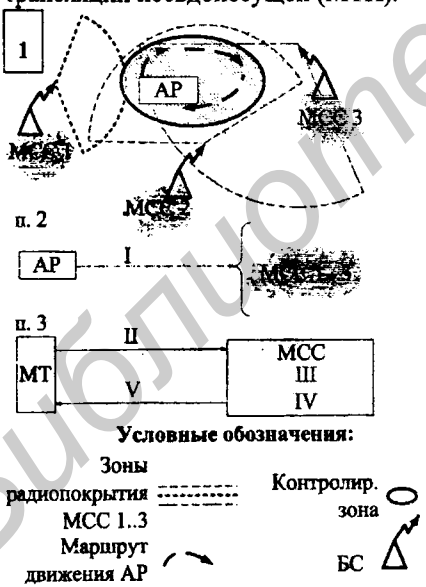

Рисунок 1 – Управление доступом на основе метода пространственной локализации

Определено, что метод на основе пространственной локализации позволяет, за счет взаимодействия с мобильными сетями, блокировать только те терминалы, координаты которых совпадают с координатами контролируемой зоны [2–А, 10–А].

На рисунке 1 показаны этапы реализации метода пространственной локализации [10–А]:

п.1 – анализ защищаемого периметра;

п.2 – обмен данными с зарегистрированными мобильными сетями и определение блокируемых терминалов;

п.3 – отказ в установлении соединения для мобильных терминалов, находящихся в контролируемой зоне;

где АР – анализатор радиопокрытия; I –передача данных о зафиксированных

координатах в каждую из сетей соответственно; II – запрос на установление соединения; III – анализ координат терминала, инициирующего соединение; IV – отказ в установлении соединения; V – уведомление об отказе в установлении соединения.

Проведенные исследования показали, что применение данного метода позволяет проводить оперативное блокирование доступа терминалов к сетям в заданном объеме без генерации сигналов подавления. Однако отсутствует возможность контроля процесса блокирования по причине того, что управление доступом мобильных терминалов зависит от особенностей функционирования мобильных сетей.

Разработан метод управления доступом мобильных терминалов к сетям GSM на основе трансляции псевдонесущей, позволяющий произвести перерегистрацию терминалов на фиктивную базовую станцию и обеспечивающий управление ими при фоновом режиме излучения сигналов [4–А]. Установлено, что этот метод позволяет реализовать скрытное и оперативное блокирование защищаемого периметра без постоянной (периодической) генерации сигналов подавления с уровнем превышающим фоновый.

Функционирование метода определяется выражением:

$$MT = \begin{cases} БЛ \text{ при } f_{оп} = f_{пн} , \\ НБ \text{ при } f_{оп} \neq f_{пн} , \end{cases} \quad (1)$$

где MT – мобильный терминал;

$f_{оп}$ – опорная нисходящая сигнальная частота для данного МТ;

$f_{пн}$ – псевдонесущая сигнальная частота;

$БЛ$ – заблокированный МТ;

$НБ$ – незаблокированный МТ.

На рисунке 2 представлены этапы реализации метода трансляции псевдонесущей: п.1 – анализ сетевой информации и уровней сигнальных несущих; п.2 – трансляция сигналов подавления и псевдонесущих частот (первичное блокирование); п.3 – выключение сигналов подавления и понижение уровня псевдонесущей до порога чувствительности (вторичное блокирование); где УСБ – устройство управления доступом; РЭ – радиоэфир; временные интервалы: А – исходный, Б – модулированный; сигнальные частоты: I – нисходящая от мобильной сети, II – восходящая к мобильной сети, III – нисходящая от устройства управления доступом, IV – восходящая к устройству управления доступом, V – подавления от устройства управления доступом.

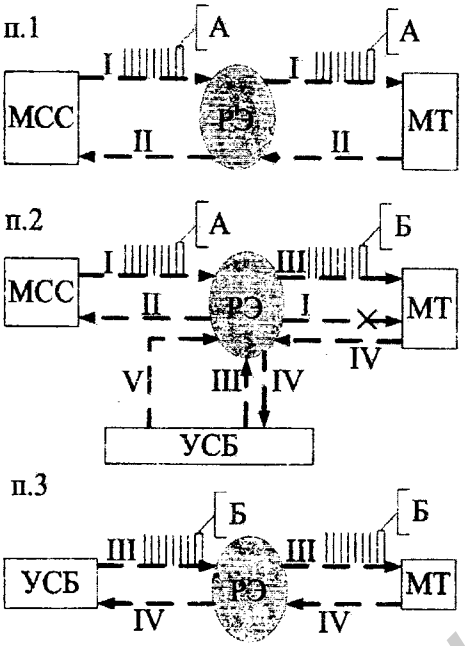

Рисунок 2 – Управление доступом на основе метода трансляции псевдонесущей

Показано, что данный метод позволяет реализовать следующие функции. 1. Контроль присутствия терминала в зоне по различным идентификаторам (MSISDN, IMSI, IMEI).

2. Избирательное управление мобильными терминалами.

3. Организация VIP-списков терминалов, связь для которых доступна в контролируемой зоне.

4. Избирательный контроль над установлением соединений.

5. Фиксация всего разрешенного трафика в контролируемой зоне.

Предложена методика системного управления доступом, согласно которой на основе данных, полученных при анализе защищаемого периметра, формируется перечень частот подавления и псевдонесущих. Сигналы подавления генерируются без информационного наполнения.

Наполнение псевдонесущих частот должно удовлетворять следующим требованиям:

1) идентификатор LA (Location Area) не должен находиться в списке запрещенных LA для роуминга;

2) идентификатор соты, передаваемый на псевдонесущей должен соответствовать принципам формирования идентификаторов в мобильных сетях;

3) сота не должна быть запрещена. При первичном блокировании включается таймер по истечении времени действия которого сигналы подавления отключаются. Это характеризует начало периода вторичного блокирования, во время которого обеспечивается контроль над терминалами до момента потери ими псевдонесущей.

Предложен алгоритм системного управления доступом мобильных терминалов к сетям GSM на основе трансляции псевдонесущей (рисунок 3), обеспечивающий блокирование терминалов до момента инициализации соединения и позволяющий понизить уровень сигнала псевдонесущей на границе

контролируемой зоны до фонового [7–А], на основе которого разработано устройство управления доступом (рисунок 4) [11–А].

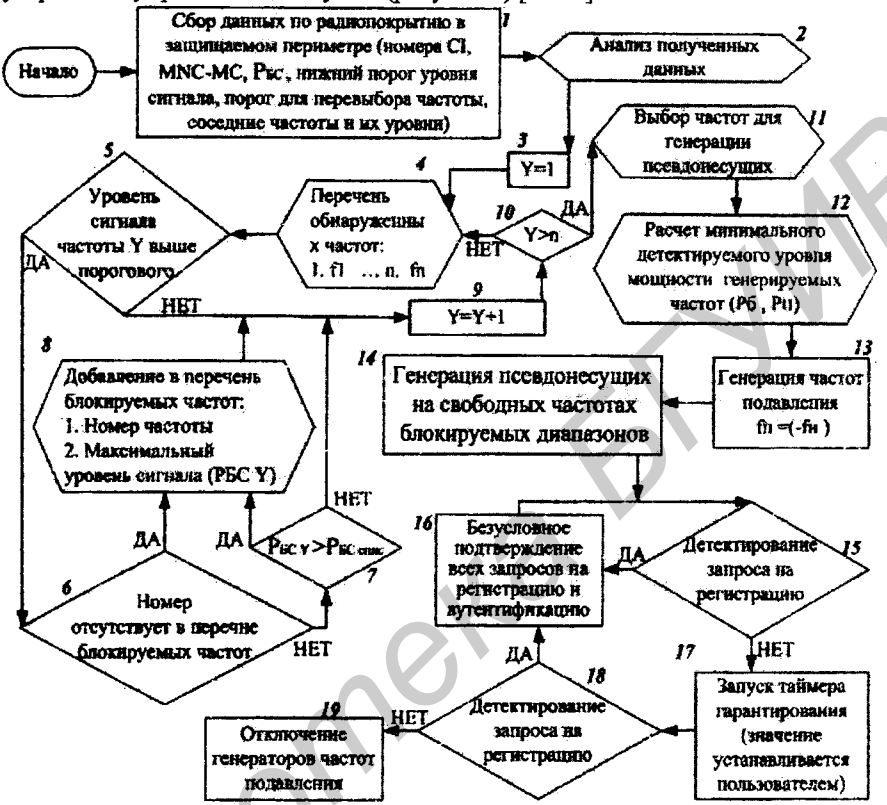

Рисунок 3 – Алгоритм управления доступом на основе метода трансляции псевдонесущей

Рисунок 4 – Структурная схема устройства управления доступом

Показано, что возможна реализация устройства управления доступом на базе передвижной (переносной) базовой станции.

Проведенные исследования показали, что вероятность блокирования для метода трансляции псевдонесущей, составляет 0,83 при нормальной нагрузке на один сигнальный канал 0,2 Эрл и минимальном размере буфера, равном одному сообщению. Установлено, что для повышения вероятности блокирования до 0,993 необходимо увеличить размер буфера до трех сообщений.

В третьей главе предложены методики оценки времени первичного блокирования мобильных терминалов, определения формируемых зон при системном блокировании и мощности транслируемых сигналов в режиме первичного блокирования.

Произведена оценка времени первичного блокирования мобильных терминалов, основанная на анализе параметров средств управления, позволяющая рассчитать продолжительность генерации сигналов подавления с учетом количества блокируемых терминалов и времени прохождения сообщений. Общее время первичного блокирования рассчитывается по формуле:

$$T = T_1 + T_2 + T_3 + T_4, \qquad (2)$$

где T_1 – время до потери несущей частоты;

T_2 – время сканирования 6-ти сигнальных частот, занесенных в память терминала;

T_3 – максимальное время цикла сканирования по диапазону;

T_4 – время для синхронизации и чтения данных на сигнальной частоте.

Показано, что для числа мобильных терминалов не более 100 и одной псевдонесущей время генерации сигналов подавления опорных несущих составляет 5 минут, вместо постоянной генерации, используемой в алгоритмах активного блокирования [6–А].

Предложена методика определения формируемых зон при управлении доступом, основанная на регистрации уровней мощности, номеров сигнальных каналов и идентификаторов сетей в защищаемом периметре, учитывающая логарифмический характер зависимости уменьшения уровня сигнала подавления от расстояния и позволяющая рассчитать границы этих зон [5–А]. Показано (рисунок 5), что при работе устройства управления доступом образуются зоны с разным соотношением уровней сигнала от базовой станции и данного устройства. В общем случае контролируемая зона будет образовывать круг с радиусом $r_{зб}$, а зона неопределенности – кольцо с шириной $\omega_{зн}$:

$$\omega_{зн} = r_{зн} - r_{зб}\ , \qquad (3)$$

где $r_{зн}$ – внешний радиус зоны неопределенности.

Радиусы $r_{зн}$, $r_{зб}$ определяются соответственно по формулам (4) и (5), в зависимости от распространения сигналов в условиях прямой видимости и при ее отсутствии:

$$\lg r = \frac{L_{los} - 42{,}64 - 20\lg f}{26}, \quad r \geq 0{,}02, \qquad (4)$$

$$25{,}6\, r + 50\lg r = L_{Nlos} - 64{,}83 - 26 \lg f, \qquad (5)$$

где r – определяемый радиус (км);

L_{los} – величина уменьшения уровня сигнала подавления для режима прямой видимости;

L_{Nlos} – величина уменьшения уровня сигнала подавления при отсутствии прямой видимости;

f – несущая частота (МГц).

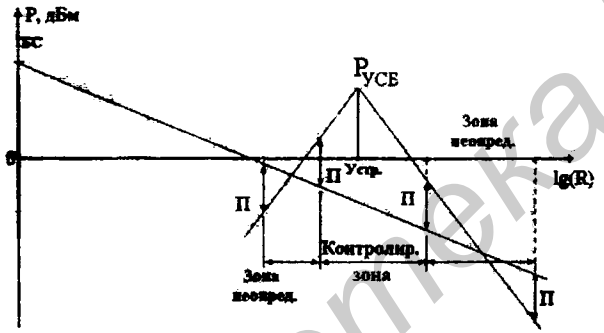

Рисунок 5 – Распределение уровней сигналов блокирования и базовой станции

Показано, что использование методики определения формируемых зон позволяет повысить точность расчета радиуса контролируемой зоны не менее, чем на 38 – 48 % по сравнению с методиками частотного подавления при мощности сигнала подавления до 4 Вт, уровне сигнала базовой станции –47 дБм и условиях прямой видимости.

Разработана методика определения мощности сигналов подавления, основанная на адаптации их уровней в зависимости от зарегистрированной максимальной мощности по каждой опорной частоте, с учетом условий распространения сигналов в контролируемой зоне. Показано, что излучаемая мощность сигнала подавления ($P_{и.\ бл}$) в период первичного блокирования рассчитывается по формуле:

$$P_{и.\ бл} = P_{БС} + П + L_1,\ П > 0,\ P_{БС} < 0, \qquad (6)$$

где $P_{БС}$ – максимальная зафиксированная мощность сигнала подавляемой опорной несущей (дБм);

$П$ – минимальный уровень превышения зафиксированной мощности (дБм);

L_1 – величина уменьшения уровня сигнала подавления до границы контролируемой зоны.

Мощность сигнала (P_n) для псевдонесущих рассчитывается по формуле:

$$P_n = \sum_{i=1}^{n} P_{БС\,i} / n \quad , \quad P'_n > P_{min} \quad , \tag{7}$$

где $P_{БС\,i}$ – максимальная зафиксированная мощность сигнала i -ой подавляемой несущей (дБм);

n – количество зафиксированных несущих;

P'_n – минимальная детектируемая мощность сигнала псевдонесущей (дБм);

P_{min} – уровень чувствительности мобильных терминалов (дБм).

В таблице 1 представлены расчеты формируемых зон для сетей GSM 900/1800 МГц при известной излучаемой мощности сигналов подавления ($P'_{и.бл}$), где радиусы контролируемой зоны: $r'_{зб}$ – в режиме прямой видимости,

Таблица 1 – Результаты расчетов формируемых зон при известной $P'_{и.бл}$ для сетей 900/1800 МГц

$P'_{и.бл}$, Вт	$P_{и.бл}$, дБм	$P_{БС}$, дБм	900 МГц				1800 МГц			
			$r'_{зб}$, м	$\omega'_{зн}$, м	$R'_{зб}$, м	$W_{зн}$, м	$r'_{зб}$, м	$\omega'_{зн}$, м	$R'_{зб}$, м	$W_{зн}$, м
1	30	-40	27	108	27	26	н/о (< 20)	58÷63	н/о (< 20)	17÷21
		-47	51	200	32	39	29	116	29	21
		-60	161	633	57	65	93	366	41	47
2	33	-40	36	140	31	30	21	81	21	21
		-47	67	261	37	44	38	151	32	26
		-60	221	826	65	72	122	477	47	53
4	36	-40	47	183	31	37	27	106	27	21
		-47	87	341	42	49	50	197	30	35
		-60	274	1077	74	80	158	622	53	60
5	37	-40	51	200	32	39	29	116	29	21
		-47	95	372	44	51	55	215	31	37
		-60	300	1177	77	83	173	679	55	63
8	39	-40	61	239	35	42	35	138	30	25
		-47	113	444	48	55	65	257	34	40
		-60	358	1405	74	99	207	811	60	67

$R'_{зб}$ – при отсутствии прямой видимости; ширина зоны неопределенности: $\omega'_{зн}$ – в режиме прямой видимости, $W_{зн}$ – при отсутствии прямой видимости.

Установлено, что при использовании метода трансляции псевдонесущей радиус зоны неопределенности для закрытых помещений в 3 раза меньше, чем для открытых территорий. Показано, что данная методика может использоваться и при оценке зон, формируемых активными блокираторами. Определено, что для мобильных сетей стандарта GSM 900/1800 МГц наименьшее соотношение контролируемой зоны и зоны неопределенности достигается при мощности сигнала подавления до 8 Вт в условиях городской застройки с радиусом контролируемой зоны до 30 м.

На рисунке 6 показаны зависимости уменьшения уровня сигнала несущей частоты от расстояния для стандарта GSM 900 МГц в режимах: отсутствия прямой видимости (L_{Nlos}), прямой видимости (L_{los}) и в свободном пространстве (L_0). Видно, что уменьшение уровня сигнала в режиме отсутствия прямой видимости происходит быстрее, чем в других режимах. На рисунке 7 представлена зависимость радиусов формируемых зон от уровня мощности сигнала базовой станции при наличии и отсутствии прямой видимости для стандарта GSM 900 МГц.

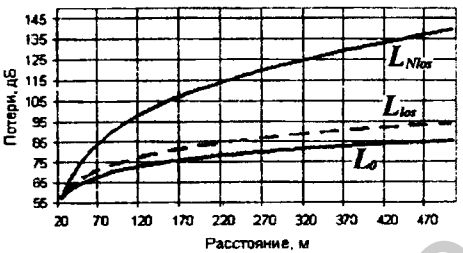

Рисунок 6 - Зависимости уменьшения уровня сигнала несущей частоты от расстояния в различных режимах

Анализ данных зависимостей показывает, что сигналы блокирования будут локализованы на открытых пространствах или вдоль «уличного каньона».

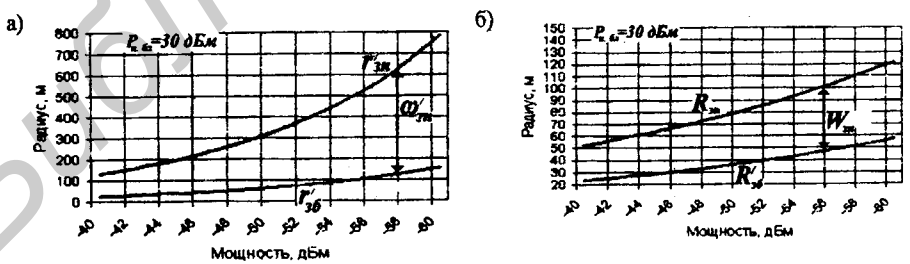

Рисунок 7 - Зависимости радиусов формируемых зон от мощности сигнала базовой станции в режимах: а) - прямой видимости и б) - отсутствия прямой видимости

В четвертой главе произведены экспериментальные исследования разработанного макета управления доступом. На рисунке 8 представлена структурная схема экспериментального макета [8–А], где 1 – анализатор радиопокрытия; 2 – устройство управления; 3 – блок формирования и преобразования; 4 – антенно-фидерный тракт; 5 – ПЭВМ управления блоком формирования и преобразования; 6 – тестовые мобильные терминалы. Эксперимент проводился для наиболее сложных условий системного блокирования – закрытого помещения с установленным технологическим оборудованием, что определило наличие многократного отражения и большого уменьшения уровня принимаемого сигнала. Разработан план эксперимента, позволяющий оценить время перехода мобильного терминала на псевдонесущую, а также радиус контролируемой зоны и минимально возможный уровень псевдонесущей. Схема движения терминала показана на рисунке 9, где 1…17 – точки измерения уровня псевдонесущей; 3*,5*,17* – точки потери псевдонесущей частоты. Результаты эксперимента подтверждают возможность реализации устройства системного блокирования, а также подтверждают соответствие расчетных и экспериментальных данных (таблица 2).

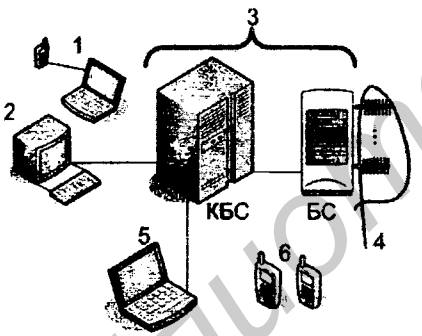

Рисунок 8 – Экспериментальный макет управления доступом

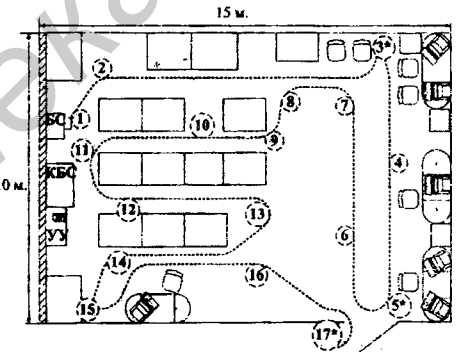

Рисунок 9– Схема движения тестового терминала при минимальном уровне псевдонесущей частоты

Установлено, что контролируемая зона равна 20 м при максимальном уровне псевдонесущей экспериментального макета в режиме первичного блокирования, равном -30 дБм и отсутствии прямой видимости. Определено, что для учета погрешности измерений из-за возможной флуктуации уровня сигнала блокируемых каналов необходимо повысить максимальное зафиксированное значение каждой опорной несущей не менее, чем на 6 дБм.

Установлено, что время перехода на псевдонесущую составляет 38 сек и не превышает расчетное (43,4 сек) при 100 % блокировании мобильных

терминалов. Проведенные исследования показали, что при системном управлении доступом мобильных терминалов к сетям GSM на основе трансляции псевдонесущей по окончании первичного блокирования излучаемый уровень на 83 дБм меньше, по сравнению с устройствами активного блокирования для радиуса контролируемой зоны 15 м.

Результаты исследований использованы УП «Агат–Систем».

Таблица 2 - Экспериментальные и расчетные данные системного управления доступом на основе трансляции псевдонесущей

№ п.п.	Показатель	Данные	
		экспериментальные	расчетные
1	Минимально возможный уровень псевдонесущей на антенне макета	-53 дБм	-
2	Минимальный уровень псевдонесущей на границе контролируемой зоны при минимальном уровне излучаемого сигнала	-109дБм	-116 дБм
3	Максимальный (эквивалентен расчетному) излучаемый уровень псевдонесущей	-30 дБм	-28 дБм
4	Минимальный уровень псевдонесущей на границе контролируемой зоны при расчетном излучаемом уровне сигнала	-87 дБм	-86 дБм
5	Время перевыбора сигнальной частоты	среднее 35,5 сек (максимальное 38 сек.).	43,4 сек
6	Время продолжительности режима первичного блокирования	5 мин	До 1мин
7	Максимальный радиус блокирования при максимальном излучаемом уровне сигнала подавления	20м (не прямая видимость)	Менее 20м (прямая видимость)
8	Уменьшение уровня сигнала псевдонесущей в контролируемой зоне	Среднее для расстояния 15м для GSM диапазона 52 дБм	Для расстояния 20м для GSM диапазона 57,55 дБм

ЗАКЛЮЧЕНИЕ

Основные научные результаты диссертации

1. Разработаны методы, алгоритмы и устройства управления доступом в мобильных сетях на основе системного блокирования, для защиты от утечки информации за пределы контролируемой зоны, включающие:

- метод, алгоритм и устройство управления доступом мобильных терминалов к сетям GSM на основе трансляции псевдонесущей, обеспечивающие блокирование терминалов до момента инициализации соединения и позволяющие понизить уровень излучаемого сигнала псевдонесущей частоты [2–А, 3–А, 8–А, 11–А];

- методику определения размеров контролируемой зоны, основанную на регистрации уровней мощности, номеров сигнальных несущих и идентификаторов сетей в защищаемом периметре, учитывающую логарифмический характер зависимости уменьшения уровня сигнала подавления от расстояния и позволяющую рассчитать границы контролируемой зоны [5–А, 6–А];

- методику определения мощности сигналов подавления в режиме первичного блокирования, основанную на адаптации их уровней в зависимости от зарегистрированной максимальной мощности по каждой опорной частоте, что позволяет снизить мощность передатчика устройства управления доступом терминалов к сетям GSM, с учетом условий распространения сигналов в контролируемой зоне [5–А, 6–А];

- методику определения времени первичного блокирования мобильных терминалов, основанную на анализе параметров канала управления и позволяющую рассчитать продолжительность генерации сигналов подавления с учетом количества терминалов и времени прохождения сообщений [6–А].

2. Впервые предложены метод, алгоритм и устройство для управления доступом мобильных терминалов к сетям GSM на основе трансляции псевдонесущей, которые позволяют понизить уровень излучаемого сигнала на 83 дБм для радиуса контролируемой зоны до 15 м по сравнению с методами частотного подавления, использующими генерацию сигналов подавления с фиксированным уровнем. Данный результат достигается за счет контроля перехода мобильных терминалов на псевдонесущую [3–А, 6–А ,8–А, 11–А].

3. Показано, что использование разработанной методики определения размеров контролируемой зоны, позволяет повысить точность расчета ее радиуса не менее чем на 38 - 48 % по сравнению с методиками частотного подавления при мощности сигнала подавления до 4 Вт, уровне сигнала базовой станции –47 дБм и условии прямой видимости. Данный результат обеспечивается за счет регистрации уровней мощности, номеров сигнальных каналов и идентификаторов сетей в защищаемом периметре [5–А, 6–А].

4. Установлено, что применение методики определения мощности сигналов подавления в режиме первичного блокирования позволяет снизить на 75% мощность передатчика устройства управления доступом терминалов к сетям GSM для обеспечения контролируемой зоны до 50 м. Данный результат достигается за счет адаптации уровней сигналов подавления по каждому каналу в зависимости от зарегистрированной максимальной мощности опорных частот с учетом условий распространения сигналов в защищаемом периметре [6–А].

5. Показано, что использование методики определения времени первичного блокирования мобильных терминалов для числа мобильных терминалов не более 100 и одной псевдонесущей позволяет сократить время генерации сигналов подавления опорных частот до 5 мин по сравнению с постоянной генерацией, используемой при активном блокировании. Данный результат обеспечивается за счет анализа параметров средств управления и расчета продолжительности генерации сигналов подавления, учитывающее количество блокируемых терминалов и время прохождения сообщений [6–А].

Рекомендации по практическому использованию результатов

1. Метод управления доступом мобильных терминалов к сетям GSM на основе трансляции псевдонесущей использован при создании экспериментального макета. Применение данного метода рекомендуется в условиях закрытых помещений, где радиус зоны неопределенности не менее, чем в 3 раза меньше по отношению к открытым территориям. Показано, что в данном случае целесообразно использовать направленные антенны [3–А, 8–А, 9–А, 11–А].

2. Метод управления доступом в мобильных сетях на основе их пространственной локализации, обеспечивающий системное блокирование доступа терминалов в защищаемом периметре без генерации сигналов подавления, за счет взаимодействия с мобильными сетями. Для его реализации следует использовать дополнительное сетевое оборудование пеленгации на каждой базовой станции или навигационные модули во всех блокируемых мобильных терминалах [2–А, 10–А].

3. Предложенная методика определения формируемых зон при системном блокировании может быть использована для расчета контролируемой зоны и зоны неопределенности при различных условиях распространения сигналов и позволяет определить радиусы этих зон с точностью до 1 м. Использование данного устройства рекомендуется для мобильных сетей стандарта GSM 900/1800 МГц при мощности сигнала подавления до 8 Вт в условиях городской застройки с радиусом контролируемой зоны до 30 м [5–А].

4. Показано, что для повышения вероятности блокирования до 0,993 по методу трансляции псевдонесущей, следует использовать буфер не менее чем для трех сообщений.

5. Рекомендуется при расчете сигналов подавления увеличить максимальное значение каждой опорной несущей не менее чем на 6 дБм, с целью учета флуктуации уровня сигналов блокируемых частот [8–А].

СПИСОК ПУБЛИКАЦИЙ СОИСКАТЕЛЯ

Статьи в научных изданиях

1–А. Галкин, А.Г. Анализ эффективности методов блокировки терминалов сотовой связи /А.Г.Галкин, В.К.Конопелько // Доклады БГУИР. – 2005. –№6. – С. 56-61.

2–А. Галкин, А.Г. Анализ возможности использования системы определения местоположения абонентов для блокирования терминалов сотовой связи. /А.Г.Галкин // Доклады БГУИР. – 2006. –№6. – С. 48-54.

3–А. Галкин, А.Г. Блокирование терминалов сотовой связи /А.Г.Галкин, В.К.Конопелько // Доклады БГУИР. – 2007. –№3. – С. 50-56.

4–А. Галкин, А.Г. Оценка общих сигнальных особенностей блокирования мобильных терминалов в сетях GSM, GPRS и EDGE /А.Г.Галкин, // Доклады БГУИР. – 2007. –№4. – С. 65-72.

5–А. Конопелько, В.К. Определение и расчет зон формируемых активными GSM блокираторами. /В.К.Конопелько, В. А. Аксенов, А.Г. Галкин// Специальная техника. - 2007. - №4. - С.48-53.

6–А. Аксенов, В. А. Временные и пространственные параметры электромагнитной обстановки при первичном блокировании терминалов GSM. /В. А. Аксенов, А.Г. Галкин // Мобильные системы . - 2007. - №8. – С.49-54.

7–А. Галкин, А.Г. Синтез системного блокиратора стандарта GSM. /А.Г.Галкин // Доклады БГУИР. – 2007 –№5 – С. 39-45.

8–А. Галкин, А.Г. Экспериментальная модель системного блокиратора стандарта GSM. /А.Г.Галкин, В. А. Аксенов // Доклады БГУИР. – 2007 –№5 – С. 46-52.

Материалы конференций

9–А. Конопелько, В.К. Межсетевые соединения в телефонии /В.К. Конопелько, А.Г. Галкин // Современные средства связи: материалы IX международной науч.-технич. конф. Известия Белорусской инженерной академии. – Минск, 2004. - №2 (18)/1. – С. 11-13.

10–А. Галкин, А.Г. Обеспечение зоны блокирования терминалов сотовой связи путем определения местоположения абонентов /А.Г. Галкин// Современные средства связи: материалы XI международной науч.-технич. конф. Нарочь, 25– 29 сентября 2006 г. / Высший государственный колледж связи; редкол.: М.А. Баркун [и др.] Минск: Бестпринт, 2006. – С. 10.

Патенты

11–А. Системный блокиратор терминалов сотовой связи узкополосных стандартов: пат. 3856 Респ. Беларусь, МПК H 04 Q 7/36 / А.Г.Галкин, В.К.Конопелько; заявитель БГУИР. – № u 20060866; заявл. 06.12.22; опубл. 30.06.04 // Афіцыйны бюл. / Нац. цэнтр інтэлектуал. уласнасці. – 2004. – № 2. – С. 174.

РЭЗЮМЭ

Галкін Андрэй Георгіевіч

КІРАВАННЕ ДОСТУПАМ Ў МАБІЛЬНЫХ СЕТКАХ НА АСНОВЕ СІСТЭМНАГА БЛАКАВАННЯ

Ключавыя словы: сістэмнае блакаванне мабільных тэрміналаў, кіраванне доступам, трансляцыя псеудаапорнай, прасторавая лакалізацыя, кантралюемая зона, зона нявызначанасці.

Мэта працы: распрацоўка метадаў, алгарытмаў і прылад кіравання доступам ў мабільных сетках на аснове сістэмнага блакавання для забеспячэння інфармацыйнай бяспекі.

Метады даследавання і апаратура: падчас даследаванняў ужываліся агульнанавуковыя метады - аналізу і сінтэзу, параўнанні, індукцыі і дэдукцыі, а таксама эксперыментальна-практычныя метады збору і апрацоўкі інфармацыі і інш.; выкарыставана наступная апаратура - аналізатар радыёпакрыцця, прылада кіравання, блок фармавання і пераўтварэнні з кіравальнай ПЭВМ, антэна-фідэрны тракт, тэставыя мабільныя тэрміналы; для апрацоўкі інфармацыі і паданні вынікаў выкарыстоўваўся стандартны пакет праграм "Microsoft Office".

Атрыманыя вынікі і іх навізна: распрацаваныя метады і алгарытмы кіравання доступам ў мабільных сетках адрозныя ад вядомых метадаў частотнага прыгнечання магчымасцю забеспячэння абмежавання доступу мабільных тэрміналаў да сеткі да моманту ўсталявання злучэння без сталай генерацыі сігналаў прыгнечання; распрацаваны - методыка азначэння магутнасці трансляваных сігналаў якая дазваляе знізіць магутнасць сігналаў прыгнечання, методыка азначэння зон, фармаваных пры сістэмным блакаванні што дазваляе разлічыць межы кантралюемай зоны і зоны нявызначанасці, методыка азначэння часу першаснага блакавання якая дазваляе разлічыць працягласць генерацыі сігналаў прыгнечання з улікам колькасці тэрміналаў і часу мінанні паведамленняў.

Рэкамендацыі па выкарыстанні: ужыванне метаду кіравання доступам мабільных тэрміналаў да сетак GSM на аснове трансляцыі псеудаапорнай рэкамендуецца ва ўмовах абмежаваных памяшканняў з выкарыстаннем накіраваных антэн; выкарыстанне метаду кіравання доступам ў мабільных сетках на аснове іх прасторавай лакалізацыі рэкамендуецца пры наяўнасці дадатковага сеткавага абсталяванне пеленгацыі на кожнай базавай станцыі або навігацыйных модуляў ва ўсіх блакаваных мабільных тэрміналах.

Вобласць ужывання: бяспека, абарона інфармацыі, кіраванне доступам.

РЕЗЮМЕ

Галкин Андрей Георгиевич

УПРАВЛЕНИЕ ДОСТУПОМ В МОБИЛЬНЫХ СЕТЯХ НА ОСНОВЕ СИСТЕМНОГО БЛОКИРОВАНИЯ

Ключевые слова: управление доступом, системное блокирование мобильных терминалов, трансляция псевдонесущей, пространственная локализация, контролируемая зона, зона неопределенности.

Цель работы: разработка методов, алгоритмов и устройств управления доступом в мобильных сетях на основе системного блокирования для обеспечения информационной безопасности.

Методы исследования и аппаратура: в процессе исследования применялись общенаучные методы – анализа и синтеза, сравнения, индукции и дедукции, а также экспериментально-практические методы сбора и обработки информации и др.; использована аппаратура включающая – анализатор радиопокрытия, устройство управления, блок формирования и преобразования с управляющей ПЭВМ, антенно-фидерный тракт, тестовые мобильные терминалы; для обработки информации и представления результатов использовался стандартный пакет программ «Microsoft Office».

Полученные результаты и их новизна: разработаны методы и алгоритмы управления доступом в мобильных сетях отличающиеся от известных методов частотного подавления возможностью обеспечения ограничения доступа мобильных терминалов к сети до момента установления соединения без постоянной генерации сигналов подавления; разработаны – методика определения мощности транслируемых сигналов позволяющую снизить мощность сигналов подавления, методика определения размеров формируемых зон при системном блокировании позволяющая рассчитать границы контролируемой зоны и зоны неопределенности, методика определения времени первичного блокирования позволяющую рассчитать продолжительность генерации сигналов подавления с учетом количества терминалов и времени прохождения сообщений.

Рекомендации по использованию: применение метода управления доступом мобильных терминалов к сетям GSM на основе трансляции псевдонесущей рекомендуется в условиях закрытых помещений с использованием направленных антенн; использование метода управления доступом в мобильных сетях на основе их пространственной локализации рекомендуется при наличии дополнительного сетевого оборудование пеленгации на каждой базовой станции или навигационных модулей во всех блокируемых мобильных терминалах.

Область применения: безопасность, защита информации, управление доступом.

SUMMARY

Halkin Andrey Georgievich

ACCESS CONTROL IN MOBILES NETWORKS ON THE BASIS OF SYSTEM BLOCKING

Key words: system blocking of mobile terminals, access control, transmition of pseudo–carrier, spatial localization, guaranteed blocking range, uncertainty range.

Object of research: is development of methods, algorithms and arrangements of access control in mobiles networks on the basis of system blocking for information security insuring.

Methods of research and the equipment: general scientific methods - the analysis and synthesis, comparison, an induction and deduction, and also experimentally-practical methods of gathering and application of the information etc.; the equipment including - the radiocovering analyzer, control unit, the block of formation and transformation with the control computer, antenna-feeder path, test mobile terminals are used; for information processing and results representation the standard software package «Microsoft Office» was used.

The received results and their novelty: developed methods and algorithms of access control in mobiles networks differ from the known methods of frequency suppression by possibility to provide access limitation of mobile terminals to a network till the moment of connection without constant generation of signals of suppression; are developed - methods of definition of broadcast signals power in a mode of primary blocking; methods of definition of formed guaranteed blocking and uncertainty ranges; methods of mobile terminals primary blocking time definition allowing to calculate time duration of suppression signals generation subject to quantity of terminals number and passage time of messages.

Recommendations on use: system blocking method of transmission and information distribution between mobile terminal and GSM network on the basis of pseudo–carrier transmition is recommended in enclosed space with directional antennas use; a method of an information security insuring on the basis of spatial localization of mobile terminals at presence additional network direction finding equipment at each base station or navigating modules in all blocked mobile terminals.

Field of application: safety, information security, access control.

Научное издание

Галкин

Андрей Георгиевич

УПРАВЛЕНИЕ ДОСТУПОМ В МОБИЛЬНЫХ СЕТЯХ НА ОСНОВЕ СИСТЕМНОГО БЛОКИРОВАНИЯ

Специальность 05.13.19 – Методы и системы защиты информации, информационная безопасность

АВТОРЕФЕРАТ
диссертации на соискание
ученой степени кандидата технических наук

Подписано в печать	22.04.2009. Формат 60x84 $^{1}/_{16}$.	Бумага офсетная.
Гарнитура «Таймс».	Печать ризографическая.	Усл. печ. л. 1,4.
Уч.-изд. л. 1,3.	Тираж 60 экз.	Заказ 277.

Издатель и полиграфическое исполнение: Учреждение образования
«Белорусский государственный университет информатики и радиоэлектроники»
ЛИ №02330/0494371 от 16.03.2009. ЛП №02330/0131666 от 30.04.2004.
220013, Минск, П. Бровки, 6.