УДК 004.728.3

Распределенная система противодействия несанкционированному доступу к информации абонентов сотовой связи

Перегудов М. А., Уманский А. Я., Жданова А. А., Храмов В. Ю.

Постановка задачи: *В настоящее время иностранная разведка, незаконные вооруженные формирования и террористические организации применяют ложные базовые станции, которые прослушивают сеансы сотовой связи, просматривают СМС-сообщения и способны блокировать сотовую связь. Отечественных средств защиты от ложных базовых станций нет.* ***Целью работы*** *является создание распределенной системы противодействия несанкционированному доступу к информации абонентов сотовой связи.* ***Используемые методы:*** *при создании предлагаемой системы использовались методы системного анализа для выявления подлежащих устранению недостатков известных из открытых источников иностранных средств защиты сетей сотовой связи от ложных базовых станций, а также методы теории алгоритмов для разработки способов обнаружения ложных базовых станций и противодействия им в режиме реального времени.* ***Новизна:*** *в отличие от аналогов предлагаемая распределенная система противодействия несанкционированному доступу к информации абонентов сотовой связи позволяет не только обнаруживать факт применения ложных базовых станций, но и блокировать технический канал утечки информации, восстанавливать защищенный канал связи и определять местоположение злоумышленника. Также отличительной особенностью предлагаемой системы является обнаружение ложных базовых станций по их местоположению.* ***Результат:*** *восстановление конфиденциальности информации за счет смены обслуживающей базовой станции в случае, если она не удовлетворяет требованиям легитимной базовой станции сотового оператора.* ***Практическая значимость:*** *применение распределенной системы противодействия несанкционированному доступу к информации абонентов сотовой связи позволит обеспечить конфиденциальность ее информации, а также исключить блокирование сотовой связи на критически важных объектах.*

Ключевые слова: *защита информации, система противодействия, сотовая связь, сеть, ложная базовая станция, абонентский терминал.*

Введение

В настоящее время сотовая связь самая распространенная из всех видов мобильной связи. Большинство людей сейчас не представляют свою жизнь без смартфона, планшета или умных часов (далее по тексту – абонентских терминалов). Эти средства как маленькие компьютеры, которые, помимо установления сотовой связи, могут подключаться к сети Интернет и уже давно заменили ручку и блокнот, диктофон, фото- и видеокамеру. Таким образом, данные устройства стали неотъемлемой частью жизни не только отдельно взятого человека, но и общества в целом.

Библиографическая ссылка на статью:
Перегудов М. А., Уманский А. Я., Жданова А. А., Храмов В. Ю. Распределенная система противодействия несанкционированному доступу к информации абонентов сотовой связи // Системы управления, связи и безопасности. 2022. № 2. С. 149-172. DOI: 10.24412/2410-9916-2022-2-149-172

Reference for citation:
Peregudov M. A., Umanskiy A. Ya., Zhdanova A. A., Khramov V. Yu. Distributed system to counter unauthorized access to cellular subscribers information. *Systems of Control, Communication and Security*, 2022, no. 2, pp. 149-172 (in Russian). DOI: 10.24412/2410-9916-2022-2-149-172

Системы сотовой связи (ССтС) применяются как для личного пользования, так и в государственных и силовых структурах, а также в промышленности, на критически важных объектах, предприятиях крупного, среднего и малого бизнеса.

Широкое применение ССтС на государственных, коммерческих и специальных объектах способствовало появлению нового вида угроз в области защиты информации. Несанкционированный доступ (НСД) третьих лиц к информации, циркулирующей в сетях сотовой связи, может повлечь за собой утрату конфиденциальной информации. В качестве третьих лиц могут выступать иностранная разведка, незаконные вооруженные формирования, террористические организации и хакеры, посягающие на личную информацию (далее по тексту – злоумышленники) [1, 2]. Причем оборудование, позволяющее обеспечить доступ к конфиденциальной информации по каналам сотовой связи, с одной стороны, продается в открытом доступе [3, 4], а, с другой стороны, его можно собрать из комплектующих, поставляемых из-за границы [5-8]. Такое оборудование имитирует работу базовых станций (БС) сотовых операторов и поэтому называется ложной базовой станцией (ЛБС). При этом злоумышленники получают возможность не только прослушивать абонентские терминалы (АТ), просматривать СМС-сообщения, но и блокировать как отдельного абонента, так и сотовую сеть в целом. Также злоумышленники имеют возможность дезинформировать абонентов сотовой связи через рассылку ложных СМС-сообщений. Последствия от деятельности злоумышленников, использующих ЛБС, заключается не только в утрате конфиденциальной информации, но и в блокировании связи на критически важных объектах при проведении террористических актов, что может привести к серьезным последствиям из-за несвоевременного реагирования на сложившуюся ситуацию.

Злоумышленники размещают ЛБС вблизи объекта воздействия. ЛБС подключаются к сети сотовой связи, считывают ее параметры и имитируют работу легитимной БС сотового оператора. При этом АТ, находящиеся в зоне обслуживания ЛБС, подключаются к этой «ловушке».

Таким образом, предотвращение НСД злоумышленников к информации абонентов сотовой связи и ее блокирования является актуальной задачей.

Анализ существующих средств противодействия несанкционированному доступу к информации абонентов сотовой связи

Сегодня большое внимание уделяется противодействию ЛБС [1, 2]. Отечественные средства защиты от ЛБС на сегодняшний день отсутствуют. Известны зарубежные средства защиты в виде специального программного обеспечения (СПО), устанавливаемого на абонентские терминалы [9-11]:

– «Eagle Security» – обнаруживает ЛБС за счет выявления несуществующих идентификаторов БС, динамически меняющихся значений *Time Advanced* (продвижение по времени) (T_a), определяющих неточное расстояние до БС, и контроля отключения БС [9];

– «Darshak» – обнаруживает ЛБС за счет контроля чрезмерной и периодической рассылки СМС-сообщений и при отсутствии шифрования в канале сотовой связи [10];
– «Android-IMSI-Catcher-Detector» – обнаруживает ЛБС за счет контроля отсутствия шифрования в радиоканале [10];
– «Snoop Snitch» – определяет угрозы утечки информации путем анализа прошивки АТ на наличие установленных патчей безопасности операционной системы [11].

Указанное СПО имеет ряд общих недостатков:
– отсутствует возможность обнаружения ЛБС, которая полностью имитирует работу БС сотовой связи;
– отсутствует возможность обнаружения ЛБС с применением механизма обнаружения по динамически меняющимся значениям T_a для подвижных (мобильных) абонентов сотовой связи;
– отсутствует возможность блокирования установленных сеансов связи с ЛБС и попыток их установления;
– отсутствует возможность восстановления защищенного канала связи;
– отсутствует возможность определения местоположения ЛБС злоумышленников для своевременного оповещения служб безопасности;
– механизмы обнаружения ЛБС функционируют только в сетях сотовой связи стандарта GSM/DCS (2G), хотя в современном мире широко применяются стандарты UMTS (3G), LTE (4G), а также внедряются ССтС пятого поколения (5G);
– отсутствует возможность взаимного оповещения между АТ, обслуживаемыми одной БС сотового оператора.

С учетом вышеизложенного возникает противоречие в практике, с одной стороны, в потребности в средствах защиты от ЛБС, и, с другой стороны, в отсутствии отечественных и недостаточной функциональности зарубежных средств защиты. При создании отечественного средства защиты от ЛБС необходимо использовать научно-технический задел иностранных средств защиты, а также разработать алгоритмы обнаружения ЛБС и противодействия им, учитывающие недостатки известных средств защиты.

Анализ существующего научно-методического аппарата обеспечения защищенности сетей сотовой связи

Вопросы противодействия компьютерным атакам рассматривались в работах Климова С.М. [12-14] и Макаренко С.И. [15, 16]. При этом особенностью рассматриваемых в этих работах компьютерных атак является их реализация на сетевом и вышестоящих уровнях эталонной модели взаимодействия открытых систем, в частности стека протоколов TCP/IP. Однако ЛБС реализуют свое воздействие на АТ только на канальном уровне сетей сотовой связи [17, 18]. Поэтому предлагаемые в [12-16] подходы к защите информационно-технических средств (ИТС) не применимы при защите от ЛБС.

В работе Бойко А.А. [19] рассматривается метод генерации тестовых информационно-технических воздействий, при реализации которых выявляются

уязвимости в сетях ИТС, в том числе на канальном уровне. Однако в этой работе методы и способы обнаружения информационно-технических воздействий и противодействия им не приводятся.

В работах [20-23] рассматривается способ обнаружения деструктивных воздействий за счет резкого снижения эффективности функционирования сетей цифровой радиосвязи. При функционировании ЛБС, полностью имитирующей легитимную БС сотового оператора, штатное функционирование сотовой сети не нарушается. Поэтому данный способ не позволяет обнаруживать ЛБС.

В работе [24] предлагают использовать для защиты от ЛБС дополнительно к долгосрочным идентификаторам АТ, новые краткосрочные идентификаторы. В [25] приводится анализ уязвимостей СМС-сообщений и голосовых вызовов с позиции их дешифрации, в [26] представлен алгоритм обнаружения ЛБС по ее мощности измеренной вблизи атакуемых АТ.

С учетом вышеизложенного возникает противоречие в науке, с одной стороны, в потребности в методическом обеспечении защиты от ЛБС, а с другой стороны в отсутствии алгоритмов противодействия ЛБС, а также алгоритмов обнаружения ЛБС, которые полностью имитируют работу БС сотового оператора.

Цель работы – создание распределенной системы противодействия НСД к информации абонентов сотовой связи.

Для достижения указанной цели необходимо решить следующие задачи:

– проанализировать уязвимости сотовой связи и процесс функционирования ЛБС;
– разработать способы обнаружения ЛБС и противодействия им с учетом недостатков технологий, используемых в известных иностранных средствах защиты.

Уязвимости сотовой связи

Анализ спецификаций стандартов ССтС GSM/DCS, UMTS и LTE [27-31] и материалов статьи [32] показывает, что такие сети имеют следующие уязвимости:

– наличие параметра, завышающего привлекательность БС сотовой связи (параметр C_2);
– отсутствие аутентификации БС с АТ;
– возможность организации сеансов связи без их шифрования или с шифрованием вскрытыми (взломанными) алгоритмами [32].

В сетях сотовой связи стандартов GSM/DCS выбор обслуживающей БС АТ осуществляется по критерию $\max\limits_{i} C_{2i}$ [27, 28], где $i = 1 \ldots I$, I – количество энергетически доступных АТ БС, C_{2i} – показатель привлекательности i-й БС.

Показатель привлекательности легитимной БС определяется по формуле [27, 28]:

$$C_{2i} = C_{1i} + O_{CROi}, \quad (1)$$

где: C_{1i} – показатель энергетической доступности АТ i-й БС; O_{CROi} – алгоритмический параметр, задаваемый оператором сотовой связи для i-й БС.

Для перехвата информации в сетях сотовой связи стандарта GSM/DCS ЛБС должна обеспечить выполнение следующего условия [27, 28]:

$$C_{2\text{ЛБС}} > \max_i C_{2i}, \quad (2)$$

где: $C_{2\text{ЛБС}}$ – максимальное значение показатель привлекательности ЛБС.

Выполнение условия (2) достигается за счет задания злоумышленником максимального значения показатель привлекательности ЛБС. Поэтому не требуется энергетического превышения по мощности сигнала ЛБС на входе АТ относительно мощности аналогичных сигналов легитимных БС, энергетически доступных для АТ.

В сетях сотовой связи стандартов UMTS и LTE выбор БС, обслуживающей АТ, осуществляется по критерию $\max_i C_{1i}$ [29-31]. В таких сетях алгоритмический показатель CRO (O_{CRO}), задаваемый оператором сотовой связи, отсутствует. Поэтому для перехвата информации в сетях сотовой связи стандартов UMTS и LTE ЛБС должна превысить по энергетике все БС, энергетически доступные для АТ:

$$C_{1\text{ЛБС}} > \max_i C_{1i}, \quad (3)$$

где: $C_{1\text{ЛБС}}$ – показатель энергетической доступности ЛБС для АТ.

В сетях сотовой связи стандартов GSM/DCS, UMTS и LTE осуществляется односторонняя аутентификация базовой станцией обслуживаемых АТ. При этом АТ не аутентифицирует обслуживающую его БС.

Для обеспечения аутентификации АТ с легитимной БС требуется выполнить следующую последовательность действий [27-31].

Шаг 1. АТ обращается к БС с запросом на обновление местоположения. Этот запрос в сетях сотовой связи используется для обновления данных сотовой сети о местонахождении АТ (в частности, его LAC (Location Area Code, код местоположения в городе) [27]. При этом АТ осуществляет данный запрос для ускорения маршрутизации вызовов и сообщений.

Шаг 2. В ответ на запрос обновления местоположения БС просит АТ идентифицировать себя, используя запрос идентификации. АТ отвечает, используя IMSI (International Mobile Subscriber Identity, идентификация международного абонента мобильной связи) [27].

Шаг 3. БС отправляет АТ специально сформированный зашифрованный пакет с известным ей содержанием. АТ в ответ на запрос БС отправляет содержание расшифрованного пакета с использованием шифрключа. БС сравнивает ответ АТ с исходным содержанием незашифрованного пакета данных. Если ответ совпадает с исходным содержанием, то БС аутентифицирует АТ и устанавливает с ним соединение.

Сети сотовой связи стандартов GSM/DCS, UMTS и LTE могут работать с шифрованием и без него [32]. При наличии шифрования используются алгоритмы A5/1 (наиболее распространенный алгоритм шифрования, который используется для шифрования канала АТ-БС), A5/2 (сильно упрощенный вариант алгоритма шифрования A5/1) и A5/3 (используется только в 3GPP (3rd Generation Partnership Project, проект партнерства третьего поколения) сетях).

№2. 2022
ISSN 2410-9916

При отсутствии шифрования в сеансе связи используется алгоритм A5/0. При этом БС оповещает АТ об использовании алгоритма A5/0. Кроме того АТ может оповещать БС об использовании алгоритма A5/0, тем самым инициируя отключение шифрования.

Функционирование ложной базовой станции

Ложной базовой станции для перехвата информации АТ необходимо установить соединение с легитимной БС и АТ, как показано на рис. 1. При этом с учетом вышеуказанных уязвимостей ЛБС необходимо обеспечить следующее [17, 18, 32]:

– превысить значение алгоритмического показателя CRO (O_{CRO}) относительно значений показателей привлекательности легитимных БС, находящихся в энергетической доступности с АТ;
– обеспечить аутентификацию ЛБС от имени легитимного АТ с легитимной БС;
– обеспечить отключение шифрования данных с легитимной БС.

Рис. 1. Перехват информации ложной базовой станцией

В настоящее время превышение значения показателя привлекательности ЛБС относительно значений показателей привлекательности легитимных БС, обеспечение аутентификации ЛБС от имени легитимного АТ с легитимной БС и отключение шифрования данных реализовано компанией «L3 Harris Technologies» в устройстве «StingRayII» [32], которое поставляется в силовые структуры США. Внешний вид устройства «StingRayII» представлен на рис. 2.

DOI: 10.24412/2410-9916-2022-2-149-172
URL: https://sccs.intelgr.com/archive/2022-02/07-Peregudov.pdf

Рис. 2. Внешний вид ложной базовой станции «StingRay II» фирмы «L3 Harris Technologies»

Ложные базовые станции также реализованы фирмой «Range Networks» в рамках проекта Open BTS (устройство «Open BTS development kit») и фирмой «Ettus Research» (на SDR-платформе разработано устройство «USRDN200») [32]. Внешний вид данных ЛБС представлен на рис. 3 и 4, соответственно.

Рис. 3. Внешний вид ложной базовой станции «Open BTS development kit» фирмы «Range Networks»

Рис. 4. Внешний вид ложной базовой станции на SDR-платформе фирмы «Ettus Research»

Применение ЛБС осуществляется по принципу «man-in-the-middle» (человек посередине) [33], при котором злоумышленник устанавливает связь между двумя сторонами, которые считают, что они непосредственно взаимодействуют друг с другом. То есть ЛБС находится между легитимной БС и АТ, причем легитимный АТ воспринимает ее как легитимную БС, а легитимная БС – как легитимный АТ.

Алгоритм обнаружения ложной базовой станции

С учетом вышеуказанных уязвимостей наиболее вероятно размещение ЛБС между имитируемой легитимной БС сотового оператора и целевыми абонентами. Причем с учетом небольших массогабаритных характеристик, а, следовательно, и энергетических возможностей ЛБС злоумышленнику придется находиться максимально близко к целевым абонентам. Исходя из этого, расстояния от целевого абонента до ЛБС и имитируемой легитимной БС сотового оператора будут отличаться. Это и является критерием обнаружения ЛБС. С учетом этого критерия обобщенный алгоритм обнаружения ЛБС [34] представлен в виде последовательности действий на рис. 5. Рассмотрим ее.

Рис. 5. Алгоритм обнаружения ЛБС злоумышленника

На шаге 1 АТ определяет эталонное расстояние до легитимной обслуживающей БС по их координатам по следующей формуле [35]:

$$D = \sqrt{(x - x_0)^2 + (y - y_0)^2}, \quad (4)$$

где: (x, y) – координаты обслуживающей легитимной БС; (x_0, y_0) – координаты АТ.

Координаты АТ можно получить, активировав GPS-приемник телефона. Координаты обслуживающей легитимной БС можно получить из базы данных координат БС сотовых операторов [36].

На шаге 2 АТ осуществляет прием сигнала обслуживающей БС.

На шаге 3 в АТ по задержке отклика от обслуживающей БС или по значению характеристики *TA* (продвижение по времени) определяют расстояние до обслуживающей БС. Причем T_a передается широковещательно БС в радиокана-

ле [35, 36]. С учетом T_a расстояние до обслуживающей БС определяется по формуле [34]:

$$D = 500T_a, \quad (4)$$

где: T_a – значение продвижения по времени, в диапазоне 1…N, N – максимальное значение T_a.

Задержка отклика от обслуживающей БС определяется также временем ожидания ответа от такой БС на запрос АТ. Например, в качестве запроса АТ может выступать запрос на получение доступа к радиосреде, определяемой основным каналом управления МССН (main control channel, основной канал управления). При этом расстояние до обслуживающей БС будет определяться по формуле [35]:

$$D = c\left(\frac{T_0}{2} - \tau\right), \quad (5)$$

где: τ – временной интервал в сотовых системах связи, равный 10 мс [27, 28]; c – скорость света, T_0 – время ожидания ответа от БС на запрос АТ.

Также расстояние до обслуживающей БС можно определить по уровню принятого сигнала от БС с учетом теории распространения радиоволн [35] и базовых значений мощности передачи БС в городе и сельской местности.

Если полученное фактическое расстояние до обслуживающей БС и ее эталонное расстояние отличаются более чем на заданное оператором значение, то обслуживающая БС является ложной, в противном случае переходят к шагу 1.

Алгоритм противодействие несанкционированному доступу к информации абонентов сотовой связи

При обнаружении ЛБС злоумышленника применяется обобщенный алгоритм противодействия НСД к информации абонента сотовой связи [37], который приведен на рис. 6.

Рис. 6. Алгоритм противодействия несанкционированному доступу к информации абонента сотовой связи

№2. 2022
ISSN 2410-9916

На шаге 1 при наличии голосовой передачи подается команда об окончании сеанса связи в соответствии со спецификациями [27-30]. Далее устанавливается запрет на АТ на инициализацию новых голосовых и текстовых передач.

На шаге 2 из списка соседних легитимных БС, находящегося в памяти АТ, АТ выбирает БС, с удовлетворяющим критерием привлекательности. В стандартах сотовой связи UMTS и LTE в качестве критерия привлекательности выступает максимальный уровень сигнала базовой станции [29, 30].

В стандартах сотовой связи GSM/DCS в качестве критерия привлекательности выступает максимальная сумма уровня сигнала БС на входе приемника АТ и алгоритмического параметра, задаваемого оператором в БС и широковещательно рассылаемого этой станцией своим абонентам [27, 28] (см. формулы (1) - (3)).

На шаге 3 АТ осуществляет смену обслуживающей БС и тем самым обеспечивается переподключение с ЛБС на БС, выбранную на шаге 2.

На шаге 4 по полученным расстояниям от АТ до ЛБС с учетом местоположения АТ определяют разностно-дальномерным методом [38] местоположение ЛБС, как показано на рис. 7. Также местоположение ЛБС возможно определить с помощью нескольких АТ аналогичным образом.

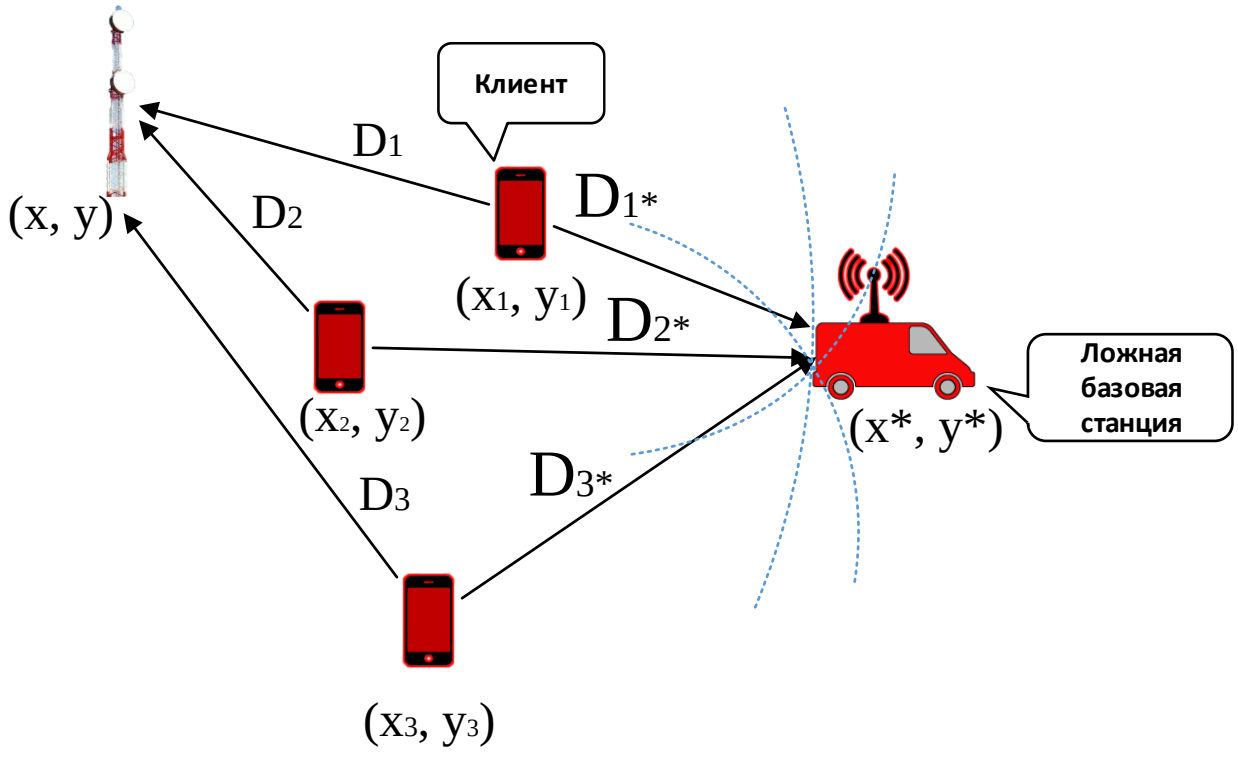

Рис. 7. Схема определения координат ложной базовой станции

Полученные координаты ЛБС могут быть переданы службам безопасности для своевременного задержания злоумышленника.

DOI: 10.24412/2410-9916-2022-2-149-172
URL: https://sccs.intelgr.com/archive/2022-02/07-Peregudov.pdf

№2. 2022
ISSN 2410-9916

Описание функционирования системы противодействия несанкционированному доступу к информации абонентов сотовой связи

Для противодействия ЛБС с учетом алгоритмов обнаружения ЛБС злоумышленника и противодействия НСД к информации абонентов сотовой связи разработан прототип системы противодействия НСД к информации абонентов сотовой связи [39-40]. Система предназначена для защиты информации, передаваемой абонентами сотовой связи, от перехвата ЛБС злоумышленника, а также для исключения блокирования злоумышленником сотовой связи.

Состав системы представлен на рис. 8. Она включает в себя клиентскую часть в виде СПО, устанавливаемого на АТ, и серверную часть, осуществляющую управление ее клиентами.

Рис. 8. Состав системы противодействия несанкционированному доступу к информации абонентов сотовой связи

Информационное взаимодействие между клиентом и сервером осуществляется в соответствии со стеком протоколов TCP/IP для взаимодействия с сетью Интернет и протоколами канального уровня сетей сотовой связи стандартов GSM/DCS, UMTS и LTE, а также протоколами канального уровня сетей широкополосного доступа семейства стандартов IEEE802.11. При этом на базе сетей сотовой связи и широкополосного доступа осуществляется доступ к сети Интернет. При таких условиях сервер, осуществляющий управление своими клиентами, сможет территориально располагаться в любой зоне, покрытой сетью Интернет. Применение резервного сервера обеспечивает бесперебойную работу в любой момент времени. В случае, если сервер недоступен клиенту, то последний, в свою очередь, работает автономно и при обнаружении ЛБС само-

DOI: 10.24412/2410-9916-2022-2-149-172
URL: https://sccs.intelgr.com/archive/2022-02/07-Peregudov.pdf

стоятельно принимает решение по противодействию НСД к информации абонента сотовой связи.

Интерфейс СПО клиента приведен на рис. 9, а интерфейс сервера – на рис. 10.

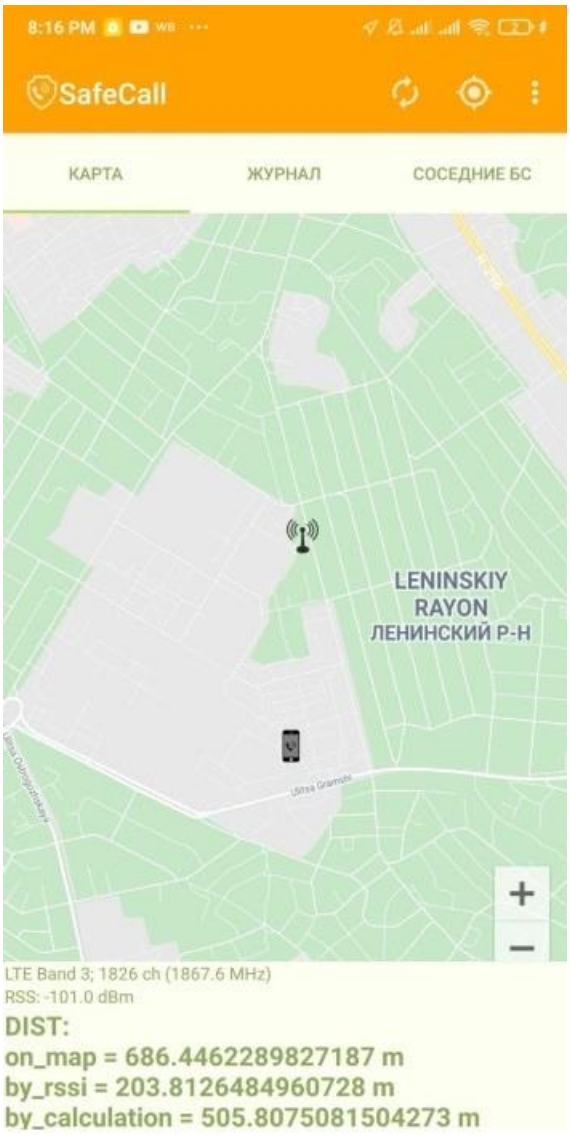

Рис. 9. Интерфейс специального программного обеспечения клиента

В состав СПО клиента и сервера входят программные средства, на которые получены свидетельства о регистрации программ для ЭВМ:

1) программный комплекс обнаружения нелегитимных БС сотовой связи [39];
2) программный модуль обнаружения НСД к информации абонента сотового телефона [40];
3) программный модуль определения расстояния до обслуживаемой БС сотовой связи [41];
4) программный модуль обработки и анализа идентификационных данных БС сотовой связи [42].

В основе системы противодействия НСД к информации абонентов сотовой связи лежат способы определения ЛБС [21] и противодействия НСД к информации абонента сотового телефона [27].

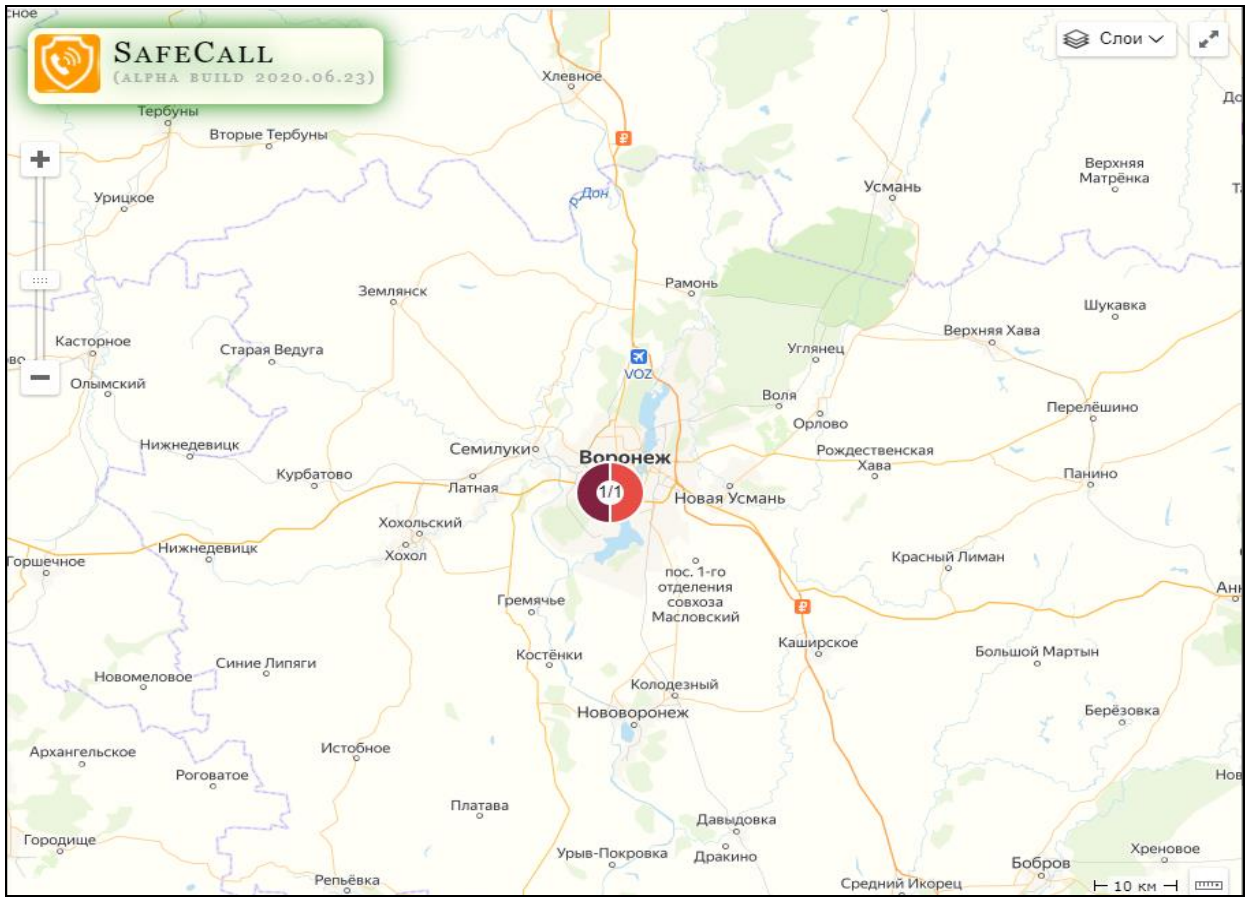

Рис. 10. Интерфейс специального программного обеспечения сервера

Этапы функционирования системы противодействия НСД к информации абонентов сотовой связи приведены на рис. 11.

В процессе радиообмена непрерывно измеряется дальность до ближайших БС сотового оператора. При появлении в системе БС на новой дальности от АТ связь с этой станцией блокируется. Обслуживание АТ передается другой БС, которая автоматически выбирается из списка в памяти АТ. После восстановления связи с БС оператора от всех клиентов, подвергшихся атаке, на сервер передается информация о дальности до ЛБС злоумышленника. При этом на сервере в реальном масштабе времени с использованием дальномерного метода определяются точные координаты злоумышленника.

Применение системы противодействия НСД к информации абонентов сотовой связи, с одной стороны, позволяет исключить блокирование сотовой связи злоумышленником, что позволяет своевременно оповестить службы безопасности, а с другой стороны, обеспечить конфиденциальность информации защищаемых объектов.

Этап 1
Обнаружение ложной базовой станции

Этап 2
Блокирование канала утечки информации абонентов сотовой связи

Этап 3
Восстановление связи с базовой станцией оператора и определение координат ложной базовой станции

Рис. 11. Этапы функционирования системы противодействия несанкционированному доступу к информации абонентов сотовой связи

Перспективы развития предлагаемой системы заключаются:
– в расширении поддерживаемых стандартов связи – до пятого поколения IMT-2020, Wi-Fi, Bluetooth;
– в расширении поддерживаемых операционных систем – до IOS, MacOS, Windows;
– в расширении поддерживаемого оборудования – до планшета, часов, ноутбука, ПК и «умного дома».

Заключение

В статье рассмотрены алгоритмы обнаружения ложных базовых станций и противодействия им в режиме реального времени. Новизной обнаружения ложных базовых станций является контроль расстояний до ближайших базовых станций сотового оператора и выявление базовых станций на новой дальности, а новизной противодействия ложным базовым станциям при их обнаружении – блокирование всех сеансов связи и попыток их установления, выбор из памяти абонентского терминала базовых станций сотового оператора и автоматическое переподключение с ложных базовых станций на выбранную базовую станцию сотового оператора. При обнаружении ложной базовой станции впервые определяются ее координаты с использованием только абонентского терминала дальномерным методом.

Новый подход к обнаружению ложных базовых станций позволяет выявить для подвижных (мобильных) абонентов сотовой связи ложные базовые станции, на 100 % имитирующих базовую станцию сотового оператора, новый подход к противодействию ложным базовым станциям – гарантированно обеспечить конфиденциальность информации абонентов сотовой связи, а реализация клиент-серверной архитектуры – осуществить возможность взаимного оповещения абонентов, обслуживаемых одной базовой станцией сотового оператора.

Предлагаемая технология построения системы противодействия несанкционированному доступу к информации абонентов сотовой связи учитывает мультистандартность (DCS/GSM, UMTS, LTE, IMT-2020, Wi-Fi, bluetooth), мультиплотформенность операционных систем (Android, IOS, macOS, Windows) и мультиплотформенность оборудования (смартфон, планшет, смарт-часы, ноутбук, персональный компьютер и «умный дом»).

В настоящее время алгоритмы обнаружения ложных базовых станций и противодействия им реализованы в прототипе системы противодействия несанкционированному доступу к информации абонентов сотовой связи. Система состоит из клиентов, устанавливаемых на абонентские терминалы, и сервера, управляющего клиентами.

Систему противодействия несанкционированному доступу к информации абонентов сотовой связи целесообразно использовать для обеспечения конфиденциальности государственной, коммерческой и личной информации, распространяемой в сетях сотовой связи на критически важных объектах, а также в промышленности и на коммерческих предприятиях.

Литература

1. Ласточкин Ю. И. Эфир под надежным контролем // Красная звезда. 2022. № 41. С. 5.

2. В Минобороны рассказали о прослушке телефонов спецслужбами стран НАТО // Рамблер [Электронный ресурс]. – URL: https://news.rambler.ru/army/48488451-v-minoborony-rasskazali-o-proslushke-telefonov-spetssluzhbami-stran-nato/ (дата обращения: 27.04.2022).

3. Другие телекоммуникационные системы // Интернет магазин «SENDLE.ru» [Электронный ресурс]. – URL: https://sendle.ru/51279-drugie-telekommunikacionnye-sistemy/223172817877-u1-rack-uran1-usrp-based-openbts-sdr-gsm-base-station-development-kit-.html (дата обращения: 03.05.2022).

4. Программно определяемое радиоустройство USRP N200 - Ettus Research // Интернет магазин «RoboticsShop» [Электронный ресурс]. – URL: https://roboticsshop.ru/parts/parts-ettus/usrp-n200 (дата обращения: 03.05.2022).

5. GSM GPRS RRU ZXG10 M8206 CTU S9000 900 МГц цифровая сотовая базовая станция // Интернет магазин «Alibaba.com» [Электронный ресурс]. – URL: https://russian.alibaba.com/p-detail/GSM-50038904423.html?spm=a2700.7724857.normal_offer.d_title.33882 72be6YpuM (дата обращения: 26.05.2022).

6. Huawei DBS3900 беспроводной GSM базовой станции DRRU3152-e DRRU3152-fa базовой станции связи оборудования // Интернет магазин «Alibaba.com» [Электронный ресурс]. – URL: https://russian.alibaba.com/p-detail/Huawei-62346045796.html?spm=a2700.7724857.normal_offer.d_image.33 88272be6YpuM (дата обращения: 26.05.2022).

7. Оригинальная Huawei DBS3900 беспроводной GSM базовой станции DRRU3152-e DRRU3152-fa базовой станции связи оборудования // Интернет магазин «Alibaba.com» [Электронный ресурс]. – URL: https://russian.alibaba.com/p-detail/Original-1600495240674.html?spm=a2700.7724857.normal_offer.d_titl e.3388272be6YpuM (дата обращения: 26.05.2022).

8. 10 портов 698-2690 МГц 11dBi двойная поляризованная направленная gsm базовая станция // Интернет магазин «Alibaba.com» [Электронный ресурс]. – URL: https://russian.alibaba.com/p-detail/10-62361331333.html?spm=a2700.7724857.normal_offer.d_title.4c77272bFq2zDK (дата обращения: 26.04.2022).

9. EAGLE Security // Oracle.com [Электронный ресурс]. – URL: https://docs.oracle.com/en/industries/communications/eagle/46.9/security-guide/eagle-security-overview.html (дата обращения: 25.04.2022).

10. Прослушивание мобильных телефонов и их защита // Habr [Электронный ресурс]. – URL: https://habr.com/ru/post/238923/ (дата обращения: 25.04.2022).

11. SnoopSnitch для Android предупреждает вас о поддельных базовых станциях // railstoolkit.ru [Электронный ресурс]. – URL: https://ru.railstoolkit.com/snoopsnitch-dlya-android-preduprezhdaet-vas-o-poddelnyh-bazo (дата обращения: 25.04.2022).

12. Климов С. М. Методы и модели противодействия компьютерным атакам. – Люберцы: Каталист, 2008. – 316 с.

13. Климов С. М., Сычев М. П., Астрахов А. В. Противодействие компьютерным атакам. Методические основы. – М.: МГТУ имени Н. Э. Баумана, 2013. – 110 с.

14. Климов С. М., Сычев М. П., Астрахов А. В. Противодействие компьютерным атакам. Технологические основы. – М.: МГТУ имени Н. Э. Баумана, 2013. – 71 с.

15. Макаренко С. И. Аудит безопасности критической инфраструктуры специальными информационными воздействиями. – СПб.: Наукоемкие технологии, 2018. – 122 с.

16. Макаренко С. И. Информационная безопасность: учебное пособие. – Ставрополь: СФ МГГУ им. М. А. Шолохова, 2009. – 372 с.

17. Бойко А. А., Гриценко С. А. Модель применения авиационного модуля нарушения доступности абонентских терминалов сотовой связи для круговой траектории полета // Вестник Воронежского государственного университета. 2013. № 2. С. 58-65.

18. Леньшин А. В., Лихачев В. П., Ханов Э. Б. Методика моделирования отношения мощностей сигналов базовой станции и блокиратора абонентских терминалов в диапазонах частот систем подвижной радиосвязи // Теория и техника радиосвязи. 2012. № 1. С. 9-12.

19. Бойко А. А. Киберзащита автоматизированных систем воинских формирований. Монография. – СПб.: Наукоемкие технологии, 2021. – 300 с.

20. Перегудов М. А., Бойко А. А. Модель процедуры зарезервированного доступа к среде сети пакетной радиосвязи // Телекоммуникации. 2015. № 6. С. 7-15.

21. Перегудов М. А., Стешковой А. С., Бойко А. А. Вероятностная модель процедуры случайного множественного доступа к среде типа CSMA/CA // Труды СПИИРАН. 2018. № 4 (59). С. 92-114. doi: 10.15622/sp.59.4.

22. Перегудов М. А., Стешковой А. С. Модель централизованной синхронизации элементов сетей цифровой радиосвязи со случайным множественным доступом к среде типа CSMA/CA // Труды СПИИРАН. 2020. Том 19. № 1. С. 128–154. doi: 10.15622/sp.2020.19.1.5.

23. Перегудов М. А., Уманский А. Я., Храмов В. Ю., Фокин А. О. Описательная модель распределенной синхронизации элементов сетей цифровой радиосвязи стандартов IEEE 802.11s и IEEE 802.11p // Успехи современной радиоэлектроники. 2021. Том 75. № 4. С. 21-31.

24. Detecting false base stations in mobile networks // Telefonaktiebolaget LM Ericsson [Электронный ресурс]. 16.05.2022. – URL: https://www.ericsson.com/en/blog/2018/6/detecting-false-base-stations-in-mobile-networks (дата обращения: 16.05.2022).

25. SMS / voice call interception with a fake base station // Stack Exchange Network [Электронный ресурс]. 16.05.2022. – URL: https://security.stackexchange.com/questions/11785/sms-voice-call-interception-with-a-fake-base-station (дата обращения: 16.05.2022).

26. Detection and Remediation of Attack by Fake Base Stations in LTE Networks // Semantic Scholar [Электронный ресурс]. 16.05.2022. – URL: https://www.semanticscholar.org/paper/Detection-and-Remediation-of-Attack-by-Fake-Base-in-Mazroa-Arozullah/4ffcb4d56f06a923044bf10dccba0df9234e8ac1 (дата обращения: 16.05.2022).

27. ETSI TS 100 550 v6.0.0 Digital cellular telecommunications system. Mobile Station - Base Station System interface. General aspects and principles (GSM 04.01), 1997. – 12 с.

28. DCS ETSI TS 100 936 v7.0.0. Technical Specification. Digital cellular telecommunications system (Phase 2+). Layer 1. General requirements (GSM 04.04), 1998. – 23 с.

29. ETSI TS 125 410 v4.1.0 (2001-06). Technical Specification. Universal Mobile Telecommunications System (UMTS). UTRAN Iu Interface: General Aspects and Principles (3GPP TS 25.410), 2001. – 26 с.

30. TS 125 410 v5.3.0 - Universal Mobile Telecommunications System (UMTS); UTRAN Iu Interface: General Aspects and Principles (3GPP TS 25.410 version 5.3.0 Release 5), 2002. – 27 с.

31. LTE 3GPP TS 36.331, Evolved Universal Terrestrial Radio Access (E-UTRA), Radio Resource Control (RRC), Protocol Specification (Release 11), 2012. – 219 с.

32. Большой FAQ по перехвату мобильной связи: IMSI-кетчеры и как от них защититься // ZTEGid [Электронный ресурс] – URL: https://ztegid.ru/blog/razblokirovka/bolshoj-faq-po-perehvatu-mobilnoj-svyazi-imsi-ketchery-i-kak-ot-nih-zashhititsya.html/ (дата обращения: 25.04.2022).

33. Атака посредника «man-in-the-middle» // Security Lab by positive technologies [Электронный ресурс]. 24.01.2022. – URL https://www.securitylab.ru/blog/company/PandaSecurityRus/351898.php (дата обращения: 25.04.2022).

34. Перегудов М. А., Уманский А. Я., Семченко И. А., Стешковой А. С., Дегтярев И. С., Щеглов А. В., Хакимов Т. М., Храмов В. Ю. Способ определения средства коммутации и управления злоумышленника // Патент на изобретение RU 2759156 C1, опубл. 09.11.2021, бюл. № 31. – URL: https://www.fips.ru/iiss/document.xhtml?faces-redirect=true&id=0db11840ba0094604fca2c93280aa81b (дата обращения 7.05.2022).

35. Долуханов М. П. Распространение радиоволн. – М.: Связь, 1972. – 336 с.

36. Местонахождение базовых станций // xinit.ru [Электронный ресурс]. – URL: https://xinit.ru/bs/ (дата обращения: 25.04.2022).

37. Ельцов О. Н., Ханов Э.Б., Перегудов М. А., Уманский А. Я., Семченко И. А., Стешковой А. С., Дегтярев И. С., Щеглов А. В. Способ противодействия несанкционированному доступу к информации абонента сотового телефона // Патент RU 2744295 C1, опубл. 05.03.2021, бюл. № 7. – URL: https://www.fips.ru/iiss/document.xhtml?faces-

redirect=true&id=ad6e6f25c8d62201eb0297ca111d3de2 (дата обращения 7.05.2022).

38. Теоретические основы радиолокации: учебное пособие для вузов / под ред. Я.Д. Ширмана. – М.: Советское радио, 1970. – 560 с.

39. Перегудов М. А., Стешковой А. С., Семченко И. А., Уманский А. Я., Дегтярев И. С., Щеглов А. В Программный комплекс обнаружения нелегитимных базовых станций сотовой связи // Свидетельство о государственной регистрации программы для ЭВМ RU 2019664527, опубл. 08.11.2019.

40. Перегудов М. А., Дегтярев И. С., Уманский А. Я., Семченко И. А., Стешковой А. С., Щеглов А. В.Программный модуль обнаружения несанкционированного доступа к информации абонента сотового телефона // Свидетельство о государственной регистрации программы для ЭВМ RU 2021619193, опубл. 07.06.2021.

41. Перегудов М. А., Дегтярев И. С., Уманский А. Я., Семченко И. А., Стешковой А. С., Щеглов А. В. Программный модуль определения расстояния до обслуживаемой базовой станции сотовой связи // Свидетельство о государственной регистрации программы для ЭВМ RU 2021619342, опубл. 08.06.2021.

42. Перегудов М. А., Дегтярев И. С., Уманский А. Я., Семченко И. А., Стешковой А. С., Щеглов А. В. Программный модуль обработки и анализа идентификационных данных базовых станций сотовой связи // Свидетельство о государственной регистрации программы для ЭВМ RU 2021619670, опубл. 15.06.2021.

References

1. Lastochkin Yu. I. Efir pod nadezhnym kontrolem [Ether under reliable control]. *Krasnaia zvezda,* 2022, no. 41, p. 5 (in Russian).

2. V Minoborony rasskazali o proslushke telefonov spetssluzhbami stran NATO [The Ministry of Defense told about the tapping of NATO countries' telephones]. *Rambler Russia*, 27.04.2022. Available at: https://news.rambler.ru/army/48488451-v-minoborony-rasskazali-o-proslushke-telefonov-spetssluzhbami-stran-nato/ (accessed 27 April 2022).

3. Drugie telekommunikatsionnye sistemy [Other telecommunications systems]. *Online store «SENDLE.ru»*. Available at: https://sendle.ru/51279-drugie-telekommunikacionnye-sistemy/223172817877-u1-rack-uran1-usrp-based-openbts-sdr-gsm-base-station-development-kit-.html (accessed 3 May 2022).

4. Programmno opredeliaemoe radioustroistvo N200 - Ettus Research [Programmable radio device USRP N200 - Ettus Research]. *Online shop «RoboticsShop»*. Available at: https://roboticsshop.ru/parts/parts-ettus/usrp-n200 (accessed 3 May 2022).

5. GSM GPRS RRU ZXG10 M8206 CTU S9000 900 MHz tsifrovaia sotovaia bazovaia stantsiia [GSM GPRS RRU ZXG10 M8206 CTU S9000 900 MHz digital cellular base station]. *Online shop «Alibaba.com»*. Available at: https://russian.alibaba.com/p-detail/GSM-

50038904423.html?spm=a2700.7724857.normal_offer.d_title.33882 72be6YpuM (accessed 26 May 2022).

6. Huawei DBS3900 besprovodnoi GSM bazovoi stantsii DRRU3152-e DRRU3152-fa bazovoi stantsii sviazi oborudovaniia [Huawei DBS3900 wireless GSM base station DRRU3152-e DRRU3152-fa base station communication equipment]. *Online shop «Alibaba.com»*. Available at: https://russian.alibaba.com/p-detail/Huawei-62346045796.html?spm=a2700.7724857.normal_offer.d_image.33 88272be6YpuM (accessed 26 May 2022).

7. Original'naia Huawei DBS3900 besprovodnoi GSM bazovoi stantsii DRRU3152-e DRRU3152-fa bazovoi stantsii sviazi oborudovaniia [Original Huawei DBS3900 wireless GSM base station DRRU3152-e DRRU3152-fa base station communication equipment]. *Online shop «Alibaba.com»*. Available at: https://russian.alibaba.com/p-detail/Original-1600495240674.html?spm=a2700.7724857.normal_offer.d_titl e.3388272be6YpuM (accessed 26 May 2022).

8. 10 portov 698-2690 MGts 11dBi dvoinaia poliarizovannaia napravlennaia gsm bazovaia stantsiia [10 ports 698-2690 MHz 11dBi double polarized directed gsm base station]. *Online shop «Alibaba.com»*. Available at: https://russian.alibaba.com/p-detail/10-62361331333.html?spm=a2700.7724857.normal_offer.d_title.4c77272bFq2zDK (accessed 26 April 2022).

9. EAGLE Security. *Oracle.com*. Available at: https://docs.oracle.com/en/industries/communications/eagle/46.9/security-guide/eagle-security-overview.html (accessed 25 April 2022).

10. Proslushivanie mobil'nykh telefonov i ikh zashchita [Tapping and protection of mobile phones]. *Habr*. Available at: URL: https://habr.com/ru/post/238923/ (accessed 25 April 2022).

11. SnoopSnitch dlia Android preduprezhdaet vas o poddel'nykh bazovykh stantsiiakh [SnoopSnitch for Android warns you about fake base stations]. *railstoolkit.ru*. Available at: https://ru.railstoolkit.com/snoopsnitch-dlya-android-preduprezhdaet-vas-o-poddelnyh-bazo (accessed 25 April 2022).

12. Klimov S. M. *Metody i modeli protivodeistviia komp'iuternym atakam* [Methods and Models of Counteracting Computer Attacks]. Lyubertsy, Catalyst Publ., 2008. 316 p. (in Russian).

13. Klimov S. M., Sychev M. P., Astrakhov A. V. *Protivodeistvie komp'iuternym atakam. Metodicheskie osnovy* [Counteracting computer attacks. Methodological bases]. Moscow, The Bauman Moscow State Technical University, 2013. 110 p. (in Russian).

14. Klimov S. M., Sychev M. P., Astrakhov A. V. *Protivodeistvie komp'iuternym atakam. Tekhnologicheskie osnovy* [Counteracting computer attacks. Technological fundamentals]. Moscow, The Bauman Moscow State Technical University, 2013. 71 p. (in Russian).

15. Makarenko S. I. *Audit bezopasnosti kriticheskoi infrastruktury spetsial'nymi informatsionnymi vozdeistviiami*. [Critical infrastructure security audit

with special information impacts]. Saint Petersburg, Naukoemkie tekhnologii, 2018. 122 p. (in Russian).

16. Makarenko S. I. *Informatsionnaia bezopasnost'* [Information security]. Stavropol, Sholokhov Moscow State University for Humanities, 2009. 372 p. (in Russian).

17. Boiko A. A., Gritsenko S. A. Model of application of aviation module violation of availability of subscriber cellular terminals for circular flight path. *Bulletin of Voronezh state technical University*, 2013, no. 2, pp. 58-65 (in Russian).

18. Len'shin A. V., Likhachev V. P., Khanov E. B. *Metodika modelirovaniia otnosheniia moshchnostei signalov bazovoi stantsii i blokiratora abonentskikh terminalov v diapazonakh chastot sistem podvizhnoi radiosviazi* [Methods of simulation of the ratio of signals of base station and blocker of subscriber terminals in frequency ranges of mobile radio communication systems]. *Radio Communication Theory and Equipment*, 2021, no. 1, pp. 9-12 (in Russian).

19. Boiko A. A. *Kiberzashchita avtomatizirovannykh sistem voinskikh formirovanii* [Cyber protection of automated systems of military formations]. Saint Petersburg, Naukoemkie tekhnologii, 2021. 301 p. (in Russian).

20. Peregudov M. A., Boiko A. A. Model of procedure for reserved access to the packet radio network environment. *Telekommunikatsii*, 2015, no. 6, pp. 7-15 (in Russian).

21. Peregudov M. A., Steshkovoi A. S., Boiko A. A. Probabilistic model of procedure of random multiple access to medium type CSMA/CA. *SPIIRAS Proceedings*, 2018, vol. 59, no. 4, pp. 92-114. doi: 10.15622/sp.59.4 (in Russian).

22. Peregudov M. A., Steshkovoi A. S. Model of centralized synchronization of digital radio network elements with random multiple access to CSMA/CA environment. *SPIIRAS Proceedings*, 2020, vol. 19, no. 1, pp. 128-154. doi: 10.15622/sp.2020.19.1.5 (in Russian).

23. Peregudov M. A., Umanskiy A. Ya., Khramov V. Yu., Fokin A. O. Descriptive model of distributed synchronization of IEEE 802.11s and IEEE 802.11p network elements. *Uspekhi sovremennoi radioelektroniki*, 2021, vol. 75, no. 4, pp. 21-31 (in Russian).

24. Detecting false base stations in mobile networks. *Telefonaktiebolaget LM Ericsson*, 16 May 2022. Available at: https://www.ericsson.com/en/blog/2018/6/detecting-false-base-stations-in-mobile-networks (accessed 16 May 2022).

25. SMS / voice call interception with a fake base station. *Stack Exchange Network*, 16 May 2022. Available at: https://security.stackexchange.com/questions/11785/sms-voice-call-interception-with-a-fake-base-station (accessed 16 May 2022).

26. Detection and Remediation of Attack by Fake Base Stations in LTE Networks. *Semantic Scholar*, 16 May 2022. Available at: https://www.semanticscholar.org/paper/Detection-and-Remediation-of-Attack-by-Fake-Base-in-Mazroa-Arozullah/4ffcb4d56f06a923044bf10dccba0df9234e8ac1 (accessed 16 May 2022).

27. ETSI TS 100 550 v6.0.0 Digital cellular telecommunications system. Mobile Station - Base Station System interface. General aspects and principles (GSM 04.01), 1997. 12 p.

28. DCS ETSI TS 100 936 v7.0.0. Technical Specification. Digital cellular telecommunications system (Phase 2+). Layer 1. General requirements (GSM 04.04), 1998. 23 p.

29. ETSI TS 125 410 v4.1.0 (2001-06). Technical Specification. Universal Mobile Telecommunications System (UMTS). UTRAN Iu Interface: General Aspects and Principles, 2001. 26 p.

30. TS 125 410 v5.3.0 - Universal Mobile Telecommunications System (UMTS); UTRAN Iu Interface: General Aspects and Principles (3GPP TS 25.410 version 5.3.0 Release 5), 2002. 27 p.

31. LTE 3GPP TS 36.331, Evolved Universal Terrestrial Radio Access (E-UTRA), Radio Resource Control (RRC), Protocol Specification (Release 11), 2012. 219 p.

32. Bol'shoi FAQ po perekhvatu mobil'noi sviazi: IMSI-ketchery i kak ot nikh zashchitit'sia [The Big FAQ for Mobile Interception: IMSI Catchers and How to Protect Against Them]. *ZTEGid*, 26 April 2022. Available at: https://ztegid.ru/blog/razblokirovka/bolshoj-faq-po-perehvatu-mobilnoj-svyazi-imsi-ketchery-i-kak-ot-nih-zashhititsya.html/ (accessed 25 April 2022).

33. Ataka posrednika «man-in-the-middle» [The attack of the mediator «man-in-the-middle»]. *Security Lab by positive technologies*, 25 April 2022. Available at: https://ru.wikipedia.org/wiki/Атака_посредника (accessed 25 April 2022).

34. Peregudov M. A., Umanskiy A. Ya., Semchenko I. A., Steshkovoi A. S., Degtiarev I. S., Shcheglov A. V., Khakimov T. M., Khramov V. Yu. *Sposob opredeleniia sredstva kommutatsii i upravleniia zloumyshlennika* [Method for determining an attacker’s switching and control tool]. Patent Russia, no. 2759156 C1, 09.11.2021.

35. Dolukhanov M. P. *Rasprostranenie radiovoln* [Radio Wave Propagation]. Moscow, Sviaz' Publ., 1972. 336 p. (in Russian).

36. Mestonakhozhdenie bazovykh stantsii [Location of base stations]. *xinit.ru*. Available at: https://xinit.ru/bs/ (accessed 25 April 2022).

37. El'tsov O. N., Khanov E. B., Peregudov M. A., Umanskiy A. Ya., Semchenko I. A., Steshkovoi A. S., Degtiarev I. S., Shcheglov A. V. *Sposob protivodeistviia nesanktsionirovannomu dostupu k informatsii abonenta sotovogo telefona* [Method for counteracting unauthorized access to information of a cellular phone subscriber]. Patent Russia, no. 2744295 C1, 05.03.2021.

38. Shirman Ia. D. *Teoreticheskie osnovy radiolokatsii* [Theoretical bases of radar]. Moscow, Sovetskoe radio Publ., 1970. p.660. (in Russian).

39. Peregudov M. A., Steshkovoi A. S., Semchenko I. A., Umanskiy A. Ya., Degtiarev I. S., Shcheglov A. V. *Programmnyi kompleks obnaruzheniia nelegitimnykh bazovykh stantsii sotovoi sviazi* [Software Complex for Detection of Illegitimate Cellular Base Stations]. The Certificate on Official Registration of the Computer Program in Russia. No. 2019664527, 08.11.2019.

40. Peregudov M. A., Degtiarev I. S., Umanskiy A. Ya., Semchenko I. A., Steshkovoi A. S., Shcheglov A. V. *Programmnyi modul' obnaruzheniia nesanktsionirovannogo dostupa k informatsii abonenta sotovogo telefona* [Software module for detecting unauthorized access to mobile phone subscriber information]. The Certificate on Official Registration of the Computer Program in Russia. No. 2021619193, 07.06.2021.

41. Peregudov M. A., Degtiarev I. S., Umanskiy A. Ya., Semchenko I. A., Steshkovoi A. S., Shcheglov A. V. *Programmnyi modul' opredeleniia rasstoianiia do obsluzhivaemoi bazovoi stantsii sotovoi sviazi* [Software module for determining the distance to a serviced cellular base station]. The Certificate on Official Registration of the Computer Program in Russia. No. 2021619342, 08.06.2021.

42. Peregudov M. A., Degtiarev I. S., Umanskiy A. Ya., Semchenko I. A., Steshkovoi A. S., Shcheglov A. V. *Programmnyi modul' obrabotki i analiza identifikatsionnykh dannykh bazovykh stantsii sotovoi sviazi* [Cellular base station identification processing and analysis software module]. The Certificate on Official Registration of the Computer Program in Russia. No. 2021619670, 15.06.2021.

Статья поступила 17 мая 2022 г.

Информация об авторах

Перегудов Максим Анатольевич – кандидат технических наук. Докторант. Военный учебно-научный центр Военно-воздушных сил «Военно-воздушная академия имени профессора Н.Е. Жуковского и Ю.А. Гагарина» (г. Воронеж). Область научных интересов: защита информации, моделирование сетей связи. E–mail: maxaperegudov@mail.ru

Уманский Аркадий Янович – старший научный сотрудник. Военный учебно-научный центр Военно-воздушных сил «Военно-воздушная академия имени профессора Н.Е. Жуковского и Ю.А. Гагарина» (г. Воронеж). Область научных интересов: оценка эффективности функционирования сети цифровой радиосвязи. E–mail: smyle2015@mail.ru

Жданова Александра Андреевна – младший научный сотрудник. Военный учебно-научный центр Военно-воздушных сил «Военно-воздушная академия имени профессора Н.Е. Жуковского и Ю.А. Гагарина» (г. Воронеж). Область научных интересов: оценка эффективности функционирования сети цифровой радиосвязи. E–mail: zhdalexandra48@mail.ru

Храмов Владимир Юрьевич – доктор технических наук. Главный научный сотрудник. Военный учебно-научный центр Военно-воздушных сил «Военно-воздушная академия имени профессора Н.Е. Жуковского и Ю.А. Гагарина» (г. Воронеж). Область научных интересов: защита информации, моделирование сетей связи. E–mail: khramovvyu@mail.ru

Адрес: 394064, Россия, г. Воронеж, ул. Ст. Большевиков, д. 54А.

Distributed system to counter unauthorized access to cellular subscribers information

M. A. Peregudov, A. Ya. Umanskiy, A. A. Zhdanova, V. Yu. Khramov

Purpose. *At present, foreign intelligence, illegal armed groups and terrorist groupsuse false base stationsthat listen to session of cellular communications, view SMS messages and block cellular communication. No domestic protection from false base stations.* ***The goal of the paper*** *is to create distributed system to counter unauthorized access to cellular subscriber's information.* ***Methods.*** *In the proposed system, systems analysis methods were used to identify shortcomings of known open sources foreign means of protecting cellular networks from false base stations, as well as methods of algorithm theory for the development of methods of detection of false base stations and their counteraction in real time.* ***Novelty.*** *Unlike analogues, the proposed distributed system for counteracting unauthorized access to information of cellular subscribers makes it possible not only to detect the use of false base stations, but also to block the technical channel of information leakage, restore secure communication channel and locate the attacker. Also distinctive feature of the system is the detection of false base stations upon the appearance of such a station at a new range.* ***Results.*** *Restoring the confidentiality of information by changing the base station if it does not meet the requirements of the legitimate base station of the cellular operator.* ***Practical relevance.*** *Application of the distributed system to counter unauthorized access to cellular subscriber's information will ensure the confidentiality of its information, as well as prevent the blocking of cellular communications at critical facilities.*

Key words*: information protection, system to counter, cellular communication, network, false base station, subscriber's terminal.*

Information about Authors

Maksim Anatolevich Peregudov – Ph.D. of Engineering Sciences. Doctoral Candidate. Zhukovsky– Gagarin Military Aviation Academy. Field of research: information security, modeling of radio network. E-mail: maxaperegudov@mail.ru

Arkadiy Yanovich Umanskiy – Senior Research Officer. Zhukovsky–Gagarin Military Aviation Academy. Field of research: digital radio communication networks functioning efficiency evaluation. E-mail: smyle2015@mail.ru

Alexandra Andreevna Zhdanova – Research Assistant. Zhukovsky–Gagarin Military Aviation Academy. Field of research: digital radio communication networks functioning efficiency evaluation. E-mail: zhdalexandra48@mail.ru

Vladimir Yurevich Khramov – Holder of an Advanced Doctorate in Engineering Sciences. Chief science officer. Zhukovsky–Gagarin Military Aviation Academy. Field of research: information security, modeling of radio network. E-mail: khramov-vyu@mail.ru

Address: Russia, 394064, Voronezh, Old Bolsheviks Street, 54A.