

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ
Федеральное государственное бюджетное образовательное учреждение
высшего образования

«ПЕНЗЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

Политехнический институт
Факультет приборостроения,
информационных технологий и
электроники

Кафедра
«Информационная безопасность
систем и технологий»

Специальность 10.05.03 –

Специализация –

Информационная безопасность
автоматизированных систем
Разработка защищенных
автоматизированных систем

ДИПЛОМНЫЙ ПРОЕКТ

на тему

КОМПЛЕКС ДЛЯ ВЫЯВЛЕНИЯ ЗАКЛАДНЫХ УСТРОЙСТВ,
РАБОТАЮЩИХ НА ЧАСТОТАХ СОТОВОЙ СВЯЗИ

Студент

 Басыров Р.А.

Руководитель

инженер по ТЗИ 2 категории АО «НПП «Рубин»

 Яшин Е.В.

Нормоконтролёр

 Фатеев А.Г.

Рецензент

начальник группы АО «НПП «Рубин»

 Безяев Д.Ю.

Работа допущена к защите (протокол заседания кафедры от 15.06.20 № 13)

Заведующий кафедрой

 С.Л. Зефирова

Работа защищена с отметкой

хорошо (протокол заседания ГЭК

от 25.06.20 № 10)

Секретарь ГЭК

 А.П. Иванов

Пенза 2020

Оглавление

Обозначения и сокращения	4
Введение.....	5
1. Обзор правовых актов в области защиты информации	7
1.1. Правовые основы защиты информации.....	7
1.2 Главные законодательные акты Российской Федерации в сфере защиты информации.....	8
2Рассмотрение основных стандартов сотовой связи	12
2.1 Первое поколение сотовой связи.....	12
2.2 Второе поколение сотовой связи	17
2.3 Третье поколение сотовой связи.....	23
2.4 Четвертое поколение сотовой связи	29
2.5 Пятое поколение сотовой связи.....	31
3 Рассмотрение источников утечки информации по каналам сотовой связи .	33
3.1Система технических средств для обеспечения функций оперативно- розыскных мероприятий.....	33
3.2 Прослушивание через оператора сотовой связи.....	33
3.3Подключение к сигнальной сети SS7	34
3.4 Поддельная базовая станция.....	35
3.5 Фемтосоты	35
3.6 Мобильный комплекс для дистанционного прослушивания каналов сотовой связи.....	35
3.7 Устройства сотовой связи	36
4Выбор оборудования для исследования канала сотовой связи	38
5Определение требований к программному обеспечениюкомплексадля выявления закладных устройств, работающих на частотах сотовой связи	43
5.1 Общие требования к программному обеспечению комплексадля выявления закладных устройств, работающих на частотах сотовой связи	43

5.2 Требования к функционалу и возможностям программного обеспечения комплекса для выявления закладных устройств, работающих на частотах сотовой связи	43
6 Выбор программного обеспечения комплекса для выявления закладных устройств, работающих на частотах сотовой связи	45
7 Описание поиска информативного сигнала по каналам сотовой связи	47
8 Структура разработанного комплекса, предназначенного для выявления закладных устройств, работающих на частотах сотовой связи	50
9 Разработка методических рекомендаций и руководства пользователя разработанного комплекса	52
9.1 Регламент применения комплекса для выявления закладных устройств, работающих на частотах сотовой связи и руководства пользователя разработанного комплекса	52
9.2 Порядок проведения проверки помещения на наличие закладных устройств, работающих на частотах сотовой связи	54
9.3 Руководство пользователя комплекса для выявления закладных устройств, работающих на частотах сотовой связи	55
10 Вредные психофизические факторы, влияющие на органы зрения специалиста по защите информации. Методы и средства физической культуры, снижающие их воздействие	62
Заключение	66
Список используемых источников	67
Приложение А. Протокол проверки ВКР на оригинальность в системе «Антиплагиат»	69

Обозначения и сокращения

AUC – authenticationcenter (центраутентификации);
BSS - basestationsystem (системабазовыхстанций);
BTS - base telecommunication station (базоваястанция);
EIR - equipment identity register (регистр идентификация абонентского оборудования);
HLR – homelocationregister(домашний регистр местоположения);
MME – mobility management entity (узелуправлениямобильностью).
MS - mobilestation (мобильнаястанция);
MSC - mobile switching center (центркоммутации);
NSS - network switching system (системакоммутации);
RNC – radionetworkcontroller (контроллерсетирадиодоступасистемы);
SDR –softwaredefinedradio (программно определяемая радиосистема);
VLR - visited location register (визитныйрегистрместоположения);
АЦП - аналого-цифровое преобразование;
БС – базовая станция;
ВКР - выпускная квалификационная работа;
ЗУ - закладочное устройство;
ПО - программное обеспечение;
ПС – подвижная станция;
ПЭВМ - персональная электронно-вычислительная машина;
СОПМ - система технических средств для обеспечения функций оперативно-розыскных мероприятий;
ТЗ - техническое задание;
ТКУИ - технический канал утечки информации.

Введение

В эпоху активного развития сотовой связи злоумышленники имеют огромный выбор методов негласного получения конфиденциальной информации путем применения устройств, работающих по широко распространенным стандартам. В связи с этим, поиск таких средств разведки является достаточно сложной задачей. Данные устройства выявляются путем выделения сигнала закладного устройства на фоне различных сигналов от других устройств сотовой связи.

Таким образом, методы и средства информационной безопасности должны обеспечивать высокую степень защиты, поскольку к ним предъявляются повышенные требования. Поэтому теоретические и практические вопросы выявления ЗУ и защиты информации от утечки по каналам сотовой связи достаточно актуальны.

Темой для выпускной квалификационной работы является «Комплекс для выявления закладных устройств, работающих на частотах сотовой связи»

В связи с недостаточным количеством предложений на рынке цена данного специализированного оборудования является крайне высокой, а существующие образцы поставляются только комплектами. Актуальным вопросом является выбор аналогов путем:

- поиска оборудования с приемлемыми характеристиками;
- уменьшения цены оборудования, входящего в состав комплекса.

1 Обзор правовых актов в области защиты информации

1. Правовые основы защиты информации

Существуют различные законодательные и нормативные акты, которые упорядочивают и регламентируют информационные отношения. Законодательные меры возлагают ответственность за нарушение установленных норм, возникающих в информационной сфере.

В РФ законодательная и нормативно правовая база включает в себя следующее:

- акты федерального законодательства:
 - Конституция РФ;
 - федеральные конституционные законы;
 - федеральные законы;
 - законы Российской Федерации;
 - указы Президента Российской Федерации;
 - постановления правительства Российской Федерации;
 - нормативные правовые акты федеральных министерств и ведомств;
- нормативные правовые акты субъектов Российской Федерации;
- нормативно - методические документы:
 - Доктрина информационной безопасности Российской Федерации;
 - приказы ФСБ.
 - методические документы, изданные государственными органами Российской Федерации;
 - руководящие документы ФСТЭК;

Главными нормативно-правовыми актами РФ, регулирующими отношения, возникающие в сфере информационной безопасности, являются Конституция РФ и Концепция национальной безопасности[2].

В статье 23 написано, что Конституцией РФ гарантирована тайна переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений. В статье 29, часть 4 говорится о том, что граждане РФ имеют «право свободно искать, получать, передавать, производить и распространять информацию любым законным способом». Также Конституцией РФ «гарантируется свобода массовой информации» (статья 29, часть 5). Конституцией РФ гарантируется доступ к информации, относящейся к категории массовой. Понятие массовой информации обозначает ту информацию, к которой имеет право получить доступ неопределенный круг лиц.

Основные задачи в области обеспечения безопасности информации определяет Концепция национальной безопасности Российской Федерации, введенная указом Президента РФ №24 от 10.01.2000 г.

По причине того, что информационные технологии постоянно улучшаются, появляются новые отношения между субъектами и объектами в информационной сфере. В связи с этим вопросы информационной безопасности, сформулированные в Концепции национальной безопасности РФ постоянно совершенствуются, благодаря чему возможно обеспечение прав и обязанностей, возникающих между сторонами информационных процессов.

1.2 Главные законодательные акты Российской Федерации в сфере защиты информации

Закон Российской Федерации от 21 июля 1993 года № 5485-1 «О государственной тайне» [3] с изменениями и дополнениями, которые внесены после его принятия. Настоящий закон регулирует отношения, которые возникают в связи с отнесением сведений к государственной тайне,

их рассекречиванием и защитой в интересах обеспечения безопасности Российской Федерации.

Закон РФ «Об информации, информационных технологиях и защите информации» ФЗ №149-ФЗ от 2006 года является одним из основных законов в сфере защиты информации и информационной безопасности. Данный законодательный акт регламентирует отношения, возникающие при формировании и использовании информационных ресурсов Российской Федерации[1].

В законе «Об информации, информационных технологиях и защите информации» перед системами обеспечения защиты информации ставятся следующие задачи:

- предотвращение утраты, утечки, хищения, несанкционированного уничтожения, искажения, модификации, несанкционированного копирования, блокирования информации, вмешательства в информацию и информационные системы;
- обеспечение полноты, достоверности, целостности информации, а также ее массивов и программных средств обработки данных, собственника информационного ресурса;
- обеспечение конституционных прав граждан на сохранение личной тайны и конфиденциальности персональной информации, которая накапливается в банках данных;
- сохранение секретности или конфиденциальности информации в соответствии с правилами, установленными действующим законодательством и другими законодательными или нормативными актами;
- соблюдение прав авторов программно-информационной продукции, которая используется в информационных системах.

Так же этот закон регламентирует права и обязанности по отношению сторон в области защиты информации. Статьи в настоящем законе обязывают владельцев информационных ресурсов обеспечивать должный уровень защиты информации ограниченного доступа. Также владелец

должен сообщать собственнику информационных ресурсов о фактах нарушения режима защиты информации ограниченного доступа.

Особое внимание необходимо уделять на то, чтобы правильно разбираться во всех аспектах законодательной базы в этой области при разработке документов и организации защиты информации ограниченного доступа.

Указ Президента РФ от 5 декабря 2016 г. № 646 “Об утверждении Доктрины информационной безопасности Российской Федерации” [2].

Настоящая Доктрина является системой взглядов на сохранение национальной безопасности Российской Федерации в информационной сфере. Под понятием информационной сферой понимается система информации, объектов информатизации, информационных систем, которые связаны с формированием и обработкой информации, информационной безопасности, а также совокупность механизмов регулирования соответствующих общественных отношений. Также в ней определены цели и задачи обеспечения безопасности информации ограниченного доступа и информационных процессов с учетом приоритетов Российской Федерации. Цели и задачи обеспечения информационной безопасности определяется на основе информационных угроз и оценки состояния информационной безопасности.

Федеральный закон от 29 июля 2004 г. № 98-ФЗ «О коммерческой тайне» [4]. Настоящий Федеральный закон регулирует отношения, которые связаны с установлением, изменением и прекращением режима коммерческой тайны в отношении информации, составляющей секрет производства. Положения настоящего Федерального закона распространяются на информацию, которая составляет коммерческую тайну, независимо от вида носителя, на котором она зафиксирована. Положения настоящего Федерального закона не распространяются на сведения, которые относятся к государственной тайне,

в отношении которой применяются положения законодательства Российской Федерации о государственной тайне[3].

2Рассмотрение основных стандартов сотовой связи

2.1 Первое поколение стандартов сотовой связи (1G)

Стандарт NMT (Nordic Mobile Telephony) был создан в 1970-х годах как первый полностью автоматический аналоговый стандарт сотовой связи. Его разработкой занимался NTA (Nordic telecommunications administrations). В его состав входили Швеция, Норвегия, Дания, Финляндия и другие страны. Эксплуатация первой сети данного стандарта началась в 1981 году [5].

NMT имеет два варианта сетей в зависимости от частотного диапазона: NMT-450 и NMT-900. Данные виды сетей имеют частотный диапазон 450 МГц и 900 МГц соответственно. NMT-900 впервые представили в 1986 году. Он имеет гораздо больше радиоканалов, чем NMT-450 [5].

Принципы архитектуры стандарта NMT были созданы к 1973 году, а в 1977 году была разработана спецификация системы базовых станций. Спецификации NMT были свободными и открытыми. Всё это позволило множеству компаний иметь возможность производить оборудование для сетей NMT и, тем самым, развивать рынок мобильной связи. Благодаря таким компаниям, как Nokia и Ericsson, стандарт NMT получил широкое распространение [5].

Впервые в 1978 году в Финляндии был произведен первый звонок по сети стандарта NMT. Несмотря на то, что NMT разрабатывали исключительно страны северной Европы (это можно понять по названию стандарта), первую в мире коммерческую сеть данного стандарта начали использовать в Саудовской Аравии 1 сентября, что было на месяц раньше, чем в Швеции. После этого сеть NMT начали эксплуатировать Норвегии в 1981 году. Следующими странами, в которых началось использование данного стандарта стали Дания и Финляндия. Наиболее широко применять сети NMT стали использовать в основном восточной и центральной Европы, таких как Швейцария, Нидерланды, Венгрия, Румыния, Чешская Республика, Словакия, Словения, Сербия, России и многие другие.

Стандарт NMT мог предоставлять только один сервис для своих

абонентов – телефонные звонки. После этого стала возможным передача данных со скоростью 1-2 кбит/сек, но широкого распространения эта услуга не получила.

Основным недостатком стандарта NMT являлось полное отсутствие шифрования данных, передаваемых по сети. В связи с этим, любой человек, имеющий простой анализатор частот мог перехватить и прочитать передаваемые данные. Помимо всего этого, в сети MNT было достаточно сложно организовать роуминг, поскольку для этого нужны были значительные ресурсы. Из-за этого соединение с другими операторами сотовой связи было очень проблематично.

Основные составными частями сети NMT являются:

- центр коммутации (MSC);
- базовая станция (BTS);
- мобильная станция (MS).

Структура сети сотовой связи стандарта NMT изображена на рисунке 1.

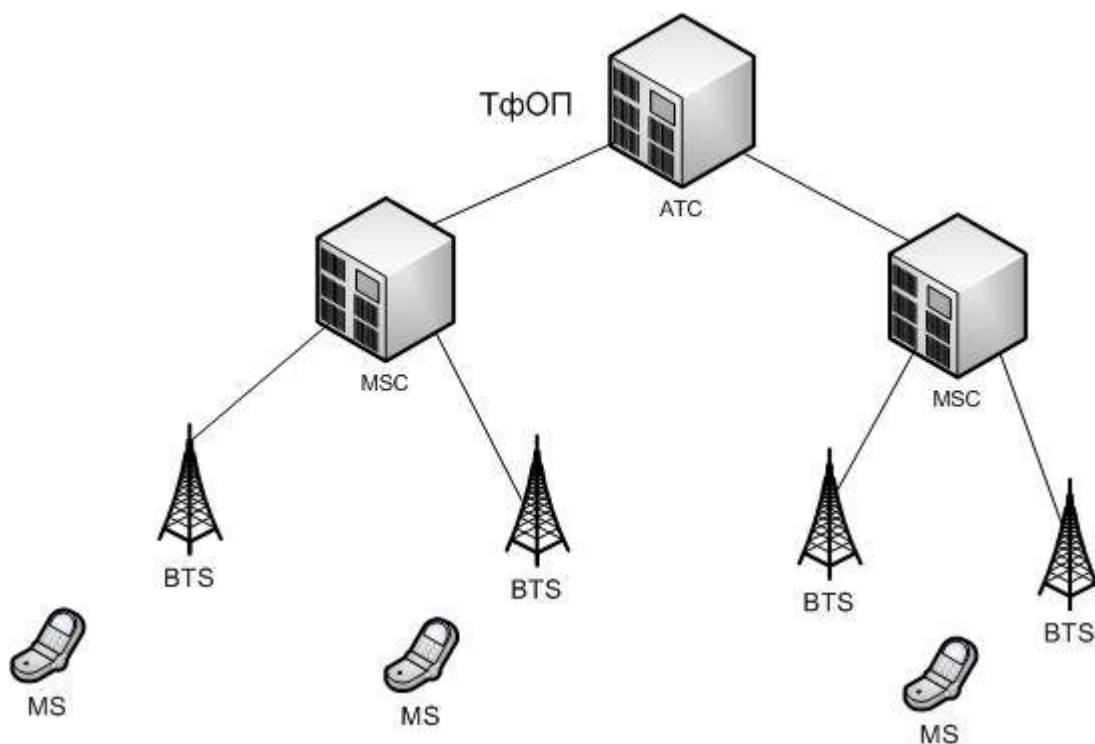


Рисунок 1 - Структура сети сотовой связи стандарта NMT

Основным элементом сети является MSC (центр коммутации

мобильной связи сети сотовой), осуществляющий управление всей системой связи стандарта NMT. Его основной задачей является установление соединения между абонентами сети, а также абонентами ТФОП. В сети оператора может быть два и более MSC. Чтобы получить обслуживание в любой точке мира данные абонента должны передаваться между коммутаторами. В центре коммутации используется регистр положения абонентов, чтобы хранить абонентские данные. В итоге при передвижении абонента данные автоматически передаются от регистра к регистру.

Базовая станция (BTS) сотовой связи создает радио покрытие на территории сот, которые располагаются поблизости. Как правило, три соты могут обслуживаться от одной БС.

Мобильной станцией (MS) является телефон абонента сотовой связи. Первые телефоны были достаточно громоздкие и кардинально отличаются от современных средств связи. Как правило, их размещали в автомобилях. Спустя некоторое время появились мобильные устройства, которые можно было удерживать в руке, но и они зачастую весили более 1 килограмма. Однако их уже можно было переносить с собой. Компактные и удобные мобильные телефоны начали появляться только в конце восьмидесятых годов прошлого века.

2.2 Второе поколение стандартов сотовой связи (2G)

D-AMPS (Digital Advanced Mobile Phone System - цифровая усовершенствованная услуга мобильной связи), иногда обозначаемая как DAMPS, является цифровой версией AMPS (усовершенствованная услуга мобильной связи), оригинального аналогового стандарта для сотовой телефонной связи в Соединенных Штатах. И D-AMPS, и AMPS сейчас используются во многих странах. D-AMPS добавляет множественный доступ с временным разделением (TDMA) к AMPS, чтобы получить три канала для каждого канала AMPS, тем самым увеличивая в три раза количество вызовов, которые могут быть обработаны в канале. D-AMPS является стандартом от Ассоциации электронной промышленности /

Ассоциации телекоммуникационной промышленности (EIA /TIA).

Как и AMPS, D-AMPS использует частотные диапазоны в пределах спектра электромагнитного излучения 800 и 900 Меггерц (МГц) . Каждый поставщик услуг может использовать половину диапазона 824–849 МГц для приема сигналов от сотовых телефонов и половину диапазона 869–894 МГц для передачи на сотовые телефоны. Полосы разделены на поддиапазоны 30 кГц , называемые каналами . Принимающие каналы называются обратными каналами, а отправляющие каналы называются прямыми каналами . Деление спектра на поддиапазонные каналы достигается с помощью частотного разделения с множественным доступом (FDMA). Обработка множественного доступа с временным разделением (TDMA) добавляется к каждому каналу поддиапазона, созданному с помощью FDMA, чтобы утроить количество доступных каналов.

Хотя AMPS и D-AMPS возникли на североамериканском рынке сотовой связи, в настоящее время они используются во всем мире с более чем 74 миллионами абонентов, по словам Ericsson, одного из крупнейших производителей сотовых телефонов. D-AMPS является одной из трех цифровых беспроводных технологий, использующих TDMA. Два других - это GSM и PDC . Каждая из этих технологий интерпретирует TDMA по-разному, поэтому они не совместимы. Преимущество D-AMPS заключается в том, что его проще обновить с существующей аналоговой сети AMPS. Альтернативой D-AMPS и двум другим технологиям TDMA является множественный доступ с кодовым разделением каналов (CDMA).

В стандарте IS-54 предусмотрено в два раза больше служебных каналов, чем в стандарте AMPS. Однако половина из них подобна набору каналов из предшествующего аналогового стандарта, т.е. используются те же протоколы и схема модуляции. Это позволяет удовлетворять принципу «обратной совместимости», который закладывался как базовое требование к системе. Основная идея заключается в том, чтобы минимизировать изменения в существующей AMPS-сети и уменьшить перерыв в

предоставлении услуг и снизить расходы на модернизацию. Принципы построения радио интерфейса стандартов AMPS и DAMPS изображены на рисунках 2 и 3.

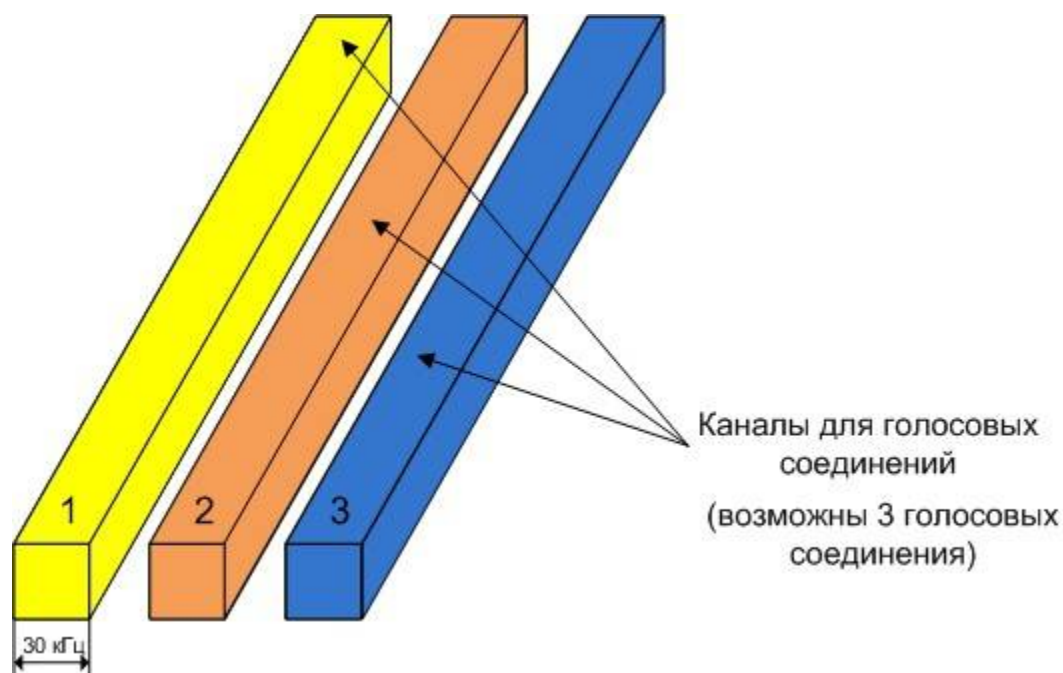


Рисунок 2 - Принцип построения радиоинтерфейса системы стандарта AMPS

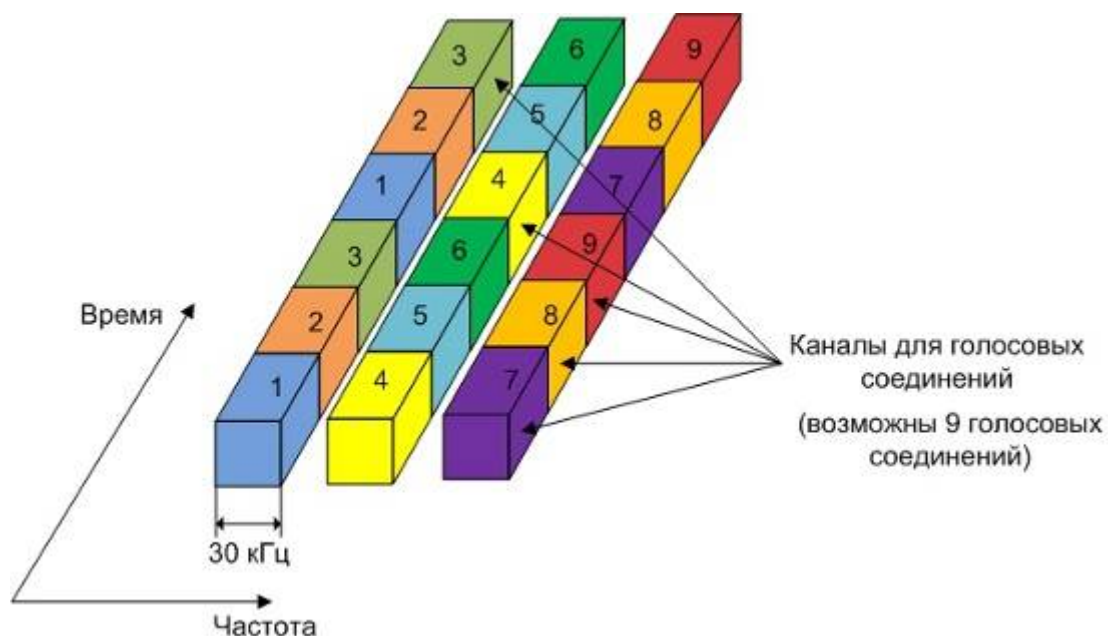


Рисунок 3 - Принцип построения радиоинтерфейса стандарта DAMPS

В стандарте D-AMPS, как было описано ранее, используется временной метод множественного доступа TDMA. Он был принят ассоциацией TTA в 1992 году. TDMA разделяет каждый частотный

FDMA-канал (30 кГц) на 3 TDMA-канала, каждый из которых способен передавать одно голосовое соединение. Позже, благодаря появившемуся новому речевому кодексу каждый из TDMA-канала так же мог быть разделен на 2 подканала, каждый из которых так же может передавать голос большей степенью сжатия. Таким образом, благодаря новому методу множественного доступа емкость сети может быть увеличена в несколько раз.

CDMA One – это первый стандарт мобильной связи, который дал толчок повсеместному использованию сотовой связи и нашел широкое распространение в Северной Америке. CDMA One – это только брендовое имя стандарта, часто упоминаемого как IS-95. Первые спецификации стандарта IS-95 выпускались под аббревиатурой IS-95A, а более поздние, усовершенствованные релизы опубликовывались как IS-95B. Именно IS-95B обычно ассоциируют с CDMA One. Наряду с речевой информацией системы сотовой связи этого стандарта могли передавать данные со скоростями: 14,4 кбит/сек для IS-95A и 115 кбит/сек - IS-95B [5].

CDMA One была первой системой сотовой связи, использующей кодовый метод множественного доступа (CDMA - code division multiple access). Предыдущие системы использовали частотный (FDMA - frequency division multiple access) и временной (TDMA - time division multiple access) методы множественного доступа. Все последующие после IS-95 стандарты сотовой связи, включая стандарты третьего поколения - 3G использовали CDMA при построении радио интерфейса. Таким образом, CDMA One оказалась первой в этой области.

Стандарт IS-95 использует кодовый принцип разделения абонентов (CDMA). Именно с его использованием связаны главные особенности и отличия от стандартов ранних поколений (NMT, AMPS, GSM и т.п.). Ключевые особенности стандарта CDMA One, которые дают преимущества перед системами других стандартов:

— мягкая передача (Soft handoff). В связи с тем, что в каждой соте используются одинаковые частоты, единственное отличие между

пользовательскими каналами заключается в использовании расширяющей последовательности. В связи с этим, при переходе абонента из одной соты в другую нет перехода между частотами, как это было в стандартах с частотным разделением. Мобильный терминал получает аналогичный сигнал, как в соте-источнике, так и в новой соте, поэтому нет необходимости в смене частоты приемника. При этом мобильный терминал может получать сигнал от двух и более сот. В связи с этим резкое снижение качества сигнала от одной соты не приведет к разрыву соединения. В свою очередь, сразу несколько базовых станций (BTS) могут принимать сигнал от MS и контроллер базовых станций (BSC) может сравнить два и более сигнала и выбрать наилучший. Оба этих фактора снижают вероятность обрыва соединения. Структура softhandoff изображена на рисунке 4;

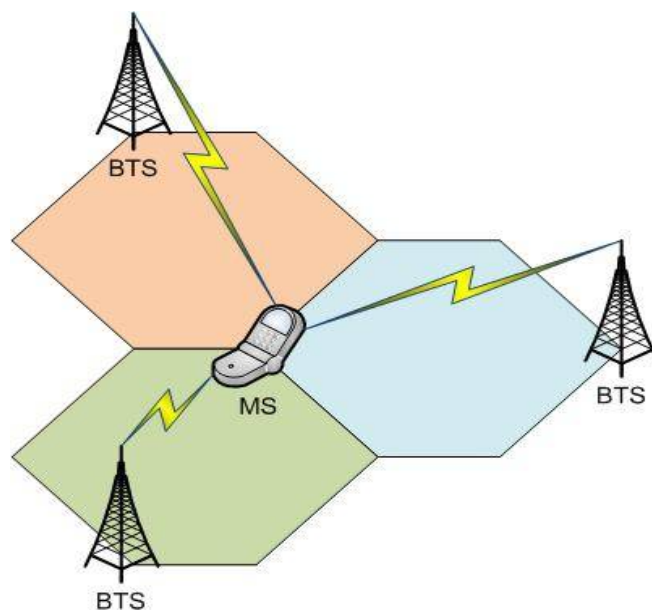


Рисунок 4 - Soft handoff с 3 базовыми станциями

— гибкая емкость сети. В системах с временным и частотным разделением строго определено количество доступных для абонентов каналов. При этом, если система настроена соответствующе и отсутствуют проблемы с работой оборудования, каналы не оказывают влияния друг на друга. Если будут попытки доступа в соту свыше числа настроенных каналов, то таким абонентам будет отказано в обслуживании. Теоретически, это не важно: разделен ли спектр на частоты, таймслоты или коды – емкость

сети будет одинаковой. Однако для CDMA все абоненты разделены с помощью кодов. Поэтому дополнительные пользователи могут быть добавлены путем небольшого снижения качества соединений. Таким образом, емкость CDMA-систем при необходимости может варьироваться;

— терпимость к многолучевому распространению. Расширение спектра эффективно в борьбе с частотно-селективными замираниями, которые могут возникать при многолучевом распространении сигналов. В случае использования CDMA, энергия полезного сигнала распределяется в широкой полосе пропускания. В связи с этим возникающие частотно-селективные замирания, которые являются сосредоточенными в узком частотном канале, не смогут внести существенных искажений для всего сигнала. Для систем, в которых энергия полезного сигнала сосредоточена в узкой области, частотно-селективные замирания могут повлечь существенное снижение качества передачи, либо даже временную блокировку каналов системы. Пример многолучевого распространения сигнала изображен на рисунке 5;

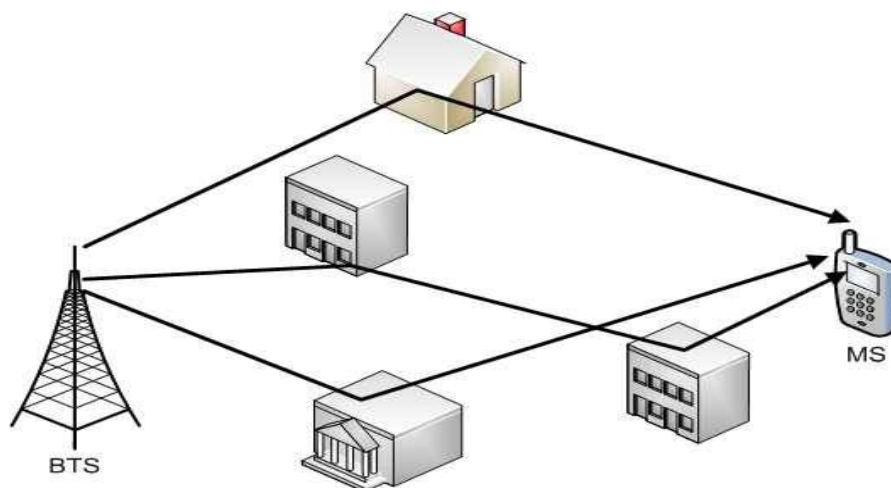


Рисунок 5 - Пример многолучевого распространения сигнала

— отсутствие необходимости использовать эквалайзер. Когда скорость передачи превышает 10 кбит/сек в FDMA и TDMA системах, необходимо использовать эквалайзер для снижения межсимвольной интерференции. По причине того, что при увеличении скорости уменьшается длительность интервала и межсимвольные интервалы,

соответственно. В связи с этим энергия последующих символов может быть наложена одна на другую. В CDMA One, за счет того что энергия каждого символа передается в широкой полосе, межсимвольная интерференция не так опасна. Кроме того, значительную помощь в борьбе с этим негативным явлением оказывает Rake-приемник;

— высокая скрытность и устойчивость к внешним воздействиям. Важная особенность расширенных сигналов заключается в том, что они становятся подобными шуму или псевдослучайными. Эти два термина значат, что спектр сигнала становится похож на спектр белого шума, как по форме, так и по мощности. Поэтому в эфире такой сигнал оказывается скрыт в покрывающих его внешних помехах и становится тяжело определить наличие сигнала и попытаться оказать на него воздействие, подслушать или подменить.

GSM - Global System for Mobile Communications (2G).

Стандарты сотовой связи второго поколения нашли широкое распространение на территории России и в других странах. Самым известным стандартом 2G является GSM (Global System for Mobile Communications - глобальная система мобильной связи). Около 80% сетей сотовой связи по всему миру построены по этому стандарту. Сети GSM используются тремя миллиардами людей более чем в 212 странах мира. Такое широкое распространение позволяет использовать международный роуминг между операторами сотовой связи, что дает возможность использовать абоненту свой телефон практически в любом уголке Земли. Причем именно возможность роуминга является главной отличительной чертой стандарта GSM от стандартов первого поколения.

Разработка стандарта GSM началась еще в 1982 году организацией по стандартизации CEPT (European Conference of Postal and Telecommunications Administrations). В 1991 году в Финляндии была введена в эксплуатацию первая в мире сеть GSM. Уже к концу 1993 года число абонентов, использующих этот стандарт, стало больше миллиона. К этому времени сети

GSM были развернуты в 73 странах мира [5].

Сети стандарта GSM позволяют предоставлять большой перечень услуг:

- голосовые соединения;
- услуги передачи данных (до 384 кбит/сек благодаря технологии EDGE);
- передача коротких текстовых сообщений (SMS);
- передача факсов;
- голосовая почта;
- конференцсвязь.

Благодаря этому GSM завоевал прочные позиции на рынке сотовой связи.

Основные элементы, входящие в состав системы GSM представлены на рисунке 6.

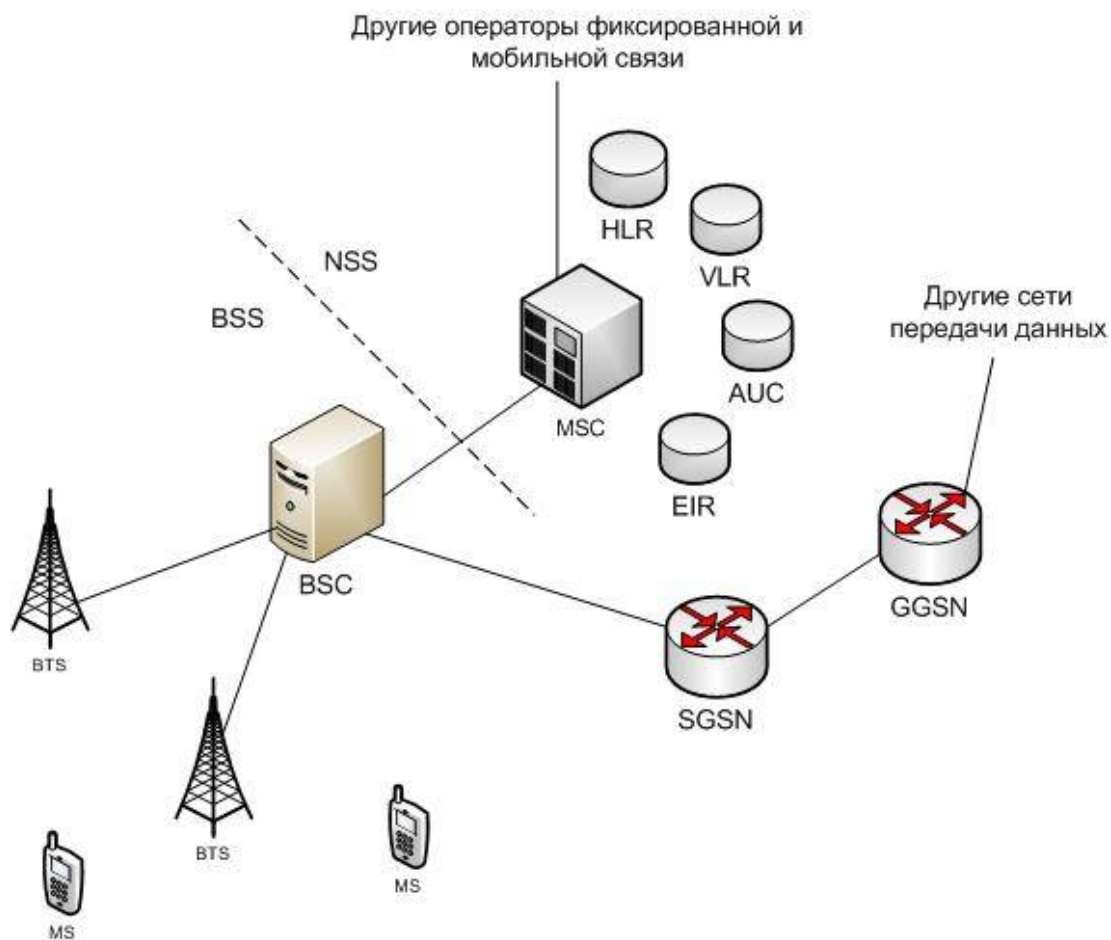


Рисунок 6 - Структура системы сотовой связи стандарта GSM

Сеть GSM делится на 2 системы. Каждая из этих систем включает в себя ряд функциональных устройств, которые, в свою очередь являются компонентами сети мобильной радиосвязи.

Данными системами являются:

- система коммутации (NSS);
- система базовых станций (BSS).

Система NSS выполняет функции обслуживания вызовов и установления соединений, а также отвечает за реализацию всех назначенных абоненту услуг. NSS включает следующие функциональные устройства:

- центр коммутации мобильной связи (MSC);
- домашний регистр местоположения (HLR);
- визитный регистр местоположения (VLR);
- центр аутентификации (AUC);
- регистр идентификация абонентского оборудования (EIR).

Система BSS выполняет все функции, относящиеся к радиоинтерфейсу. Эта система включает в себя следующие функциональные блоки:

- контроллер базовых станций (BSC);
- базовую станцию (BTS).

Состав системы коммутации NSS:

— центр коммутации мобильной связи (MSC) является главным элементом системы GSM, он осуществляет контроль за BTS и BSC, расположенные в его зоне обслуживания. Основная функция MSC заключается в установлении соединения между абонентами сети. Через него также осуществляется выход на другие сети связи: стационарную телефонную сеть, сети междугородной связи, другие сотовые сети;

— домашний регистр местоположения (HLR) содержит информацию об абонентах, которые приписаны к данному MSC. В нем хранится информация о подключенных услугах, о его состоянии (включен,

выключен, активное соединение), местоположении абонента и некоторая другая информация. Информация о каждом абоненте храниться лишь в одном HLR;

— визитный регистр местоположения (VLR) хранит информацию об активных абонентах, которые находятся в зоне обслуживания данного MSC. В него введены данные и о домашних абонентах, приписанных к данному MSC и о так называемых роумерах – абонентах, для которых данный MSC гостевой. Это могут быть абоненты других операторов связи, либо абоненты того же оператора, но из других регионов. В VLR информация поступает из HLR;

— центр аутентификации (AUC) предназначен для аутентификации абонентов. Эта процедура предназначена для предотвращения несанкционированного доступа в сеть. Каждый раз, когда абонент включает свой телефон, совершает голосовой вызов, отправляет SMS и т.п. сеть предлагает пройти процедуру аутентификации. Ее осуществляет MSC на основании данных полученных из AUC и от MS;

— регистр идентификации абонентского оборудования (EIR) является базой данных, содержащей информацию о идентификационных номерах мобильных телефонов GSM. Данная информация необходима для осуществления блокировки краденых устройств. EIR не является обязательным элементом сети. В мире есть лишь несколько операторов, которые внедрили его в своей сети.

2.3 Третье поколение стандартов сотовой связи (3G)

Стандарт CDMA2000 – это представитель стандартов сотовой связи третьего поколения (3G). Он также известен под названиями IMT-CDMA Multi-Carrier или IS-2000. Основной целью создания CDMA2000 было увеличение пропускной способности и максимально разрешенных скоростей передачи данных, по сравнению с предшествующим стандартом CDMA One. Разработка CDMA2000 началась в 2000 году, организацией 3GPP2. В итоге был выпущен целый набор стандартов,

описывающих новый радио интерфейс и значительные улучшения в сети радио доступа (Radio Access Network, RAN) и системе коммутации (CN), которые позволили добиться указанных выше требований. Таким образом, CDMA2000 – это технология, которая обеспечила эволюцию сетям CDMAOne/IS-95 к стандартам третьего поколения [5].

CDMA2000 может быть рассмотрен в нескольких фазах. Первая фаза: CDMA2000 1x, который поддерживает среднюю скорость передачи данных 144 кбит/сек. Следующей фазой является стандарт, получивший аббревиатуру: 1x-EV-DO (evolution data only or data optimised). Он позволяет передавать данные со скоростью до 2Мбит/сек на одной несущей частоте. Последним разрабатываемым стандартом серии CDMA2000 является 1x-EV-DV (Evolution Data/Voice). Он предусматривает скорости передачи данных до нескольких десятком Мбит/сек, а также улучшения в качестве передачи данных.

В стандарте CDMA One данные передавались по тем же системам, что и голос. Это значительно ограничивало максимальную скорость передачи данных и общую емкость сети. В стандарте CDMA2000 была введена специальная сеть для передачи данных: Packet Core Network (PCN) – сеть с коммутацией пакетов, которая позволяет передавать данные с большей скоростью и безопасностью.

Также как и CDMA One стандарт CDMA2000 использует для работы тот же частотный диапазон, разделенный на аналогичные полосы частот 1,25 МГц. Это значительно облегчает переход операторов к новому стандарту, так как отпадает необходимость в приобретении новой частотной лицензии, что является одним из основных сдерживающих факторов в развертывании сетей нового стандарта. Благодаря подобной преемственности операторы могут постепенно замещать оборудование более новым и тем самым снизить до минимума проблемы, возникающие при обновлении стандарта, такие как низкая распространенность абонентского оборудования, большие первоначальные затраты, организация транспортных каналов и т.п.

Стандарт CDMA2000 улучшает показатель спектральной эффективности, т.е. эффективности использования частотных ресурсов за счет следующих улучшений:

- усовершенствованный алгоритм управления мощностью. Стандарт CDMA2000 использует кодовый метод доступа абонентов в сеть – CDMA (code division multiple access). Главным недостатком является возникновение интерференции при увеличении числа абонентов. Однако благодаря механизму управления мощности для каждого мобильного терминала (MS) будет задана оптимальная мощность на данный момент времени, которая позволит с одной стороны не препятствовать другим абонентам, а с другой – обеспечить требуемый уровень качества обслуживания (QoS). Основным изменением в алгоритме управления мощностью MS стало увеличения частоты (до 16 раз) отправки команд на изменения мощности передачи данных абонентского оборудования. Благодаря этому удалось в 1,5 раза увеличить емкость сети;

- разнесенная передача (Transmit diversity) – каждая антенна имеет возможность принимать/передавать до 6 различных сигналов. При этом MS выбирает частоту с наибольшим уровнем сигнала. Благодаря Transmit diversity можно значительно снизить уровень ошибок в канале связи и увеличить качество сигнала;

- умные антенны (Smart Antennas). Они позволяют формировать отдельные пучки сигнала для каждого абонента с точностью в несколько десятков метров. Благодаря Smart antenna реализован так называемый пространственный метод множественного доступа абонентов (SDMA - Space Division Multiple Access). Это позволяет значительно снизить общий уровень интерференции в радио эфире и существенно расширить емкость сети.

UMTS - Universal Mobile Telecommunications System (3G).

Стандарты третьего поколения пришли на смену стандартам 2G. В первую очередь их появление обусловлено возросшими потребностями абонентов в скорости передачи данных. Стандарт UMTS (Universal Mobile

Telecommunications System - Универсальная система мобильной связи) нашел наибольшее распространение среди других стандартов этого поколения на территории Европы, в том числе и России.

Разработка стандарта UMTS началась в 1992 году организацией по стандартизации IMT-2000. Впоследствии разработка этого стандарта была поручена 3GPP. Первая сеть UMTS была запущена в коммерческую эксплуатацию 1 декабря 2001 года в Норвегии. К маю 2010 года число абонентов переваливает за 540 миллионов по всему миру.

Скорость передачи данных для сетей UMTS может достигать 2Мбит/сек. Благодаря технологии HSDPA-High Speed Downlink Packet Access (3.5G), которая была внедрена в 2006 году максимальная скорость возросла до 14 Мбит/сек. Эти и другие преимущества UMTS позволяют предоставлять абонентам широкий перечень услуг: видеозвонки, видеоконференции, высококачественные голосовые звонки, загрузка файлов с высокой скоростью, сетевые игры, мобильная коммерция и многое другое [5].

Структура системы UMTS и ее основные отличия от стандарта второго поколения GSM представлены на рисунке 7.

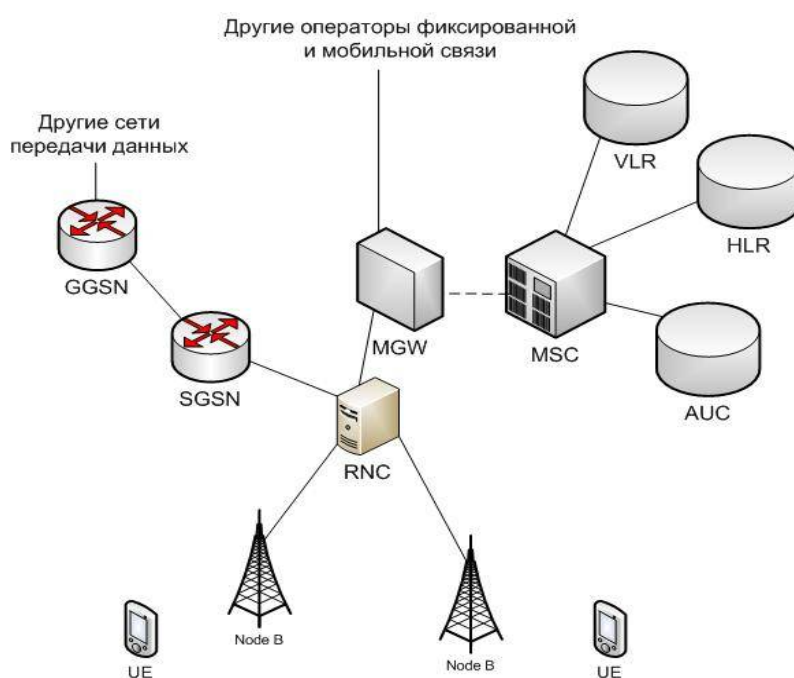


Рисунок 7 - Структура сети стандарта UMTS

Подсистема коммутации.

В первых релизах стандарта UMTS (R99, R4) подсистема коммутации не отличалась по своей структуре от той же подсистемы сетей второго поколения. В нее входили MSC – Mobile Switching Centre, который выполнял функции коммутации, установления соединения, тарификации и др., а также ряд регистров HLR, VLR, AUC, которые предназначены для хранения абонентских данных. В более поздних релизах (R5, R6, R7, R8) функции MSC были разделены между двумя устройствами: MSC-Server и MGW (Media gateway). MSC-Server отвечает за установление соединений, тарификацию, выполняет некоторые функции аутентификации. MGW представляет собой коммутационное поле, подчиненное MSC-Server.

Подсистема базовых станций.

В сети UMTS по сравнению с сетью GSM наибольшие изменения претерпела подсистема базовых станций. Данные преимущества достигаются в первую очередь за счет новой технологии передачи информации между базовой станцией и телефоном абонента.

Основные элементы, входящие в подсистему базовых станций:

— RNC (Radio Network Controller) – контроллер сети радиодоступа системы UMTS. Он является центральным элементом подсистемы базовых станций и выполняет большую часть функций: контроль радиоресурсов, шифрование, установление соединений через подсистему базовых станций, распределение ресурсов между абонентами и др. В сети UMTS контроллер выполняет гораздо больше функций нежели в системах сотовой связи второго поколения;

— NodeB – базовая станция системы сотовой связи стандарта UMTS. Основной функцией NodeB является преобразование сигнала, полученного от RNC в широкополосный радиосигнал, передаваемый к телефону. Базовая станция не принимает решений о выделении ресурсов, об изменении скорости к абоненту, а лишь служит мостом между контроллером

и оборудованием абонента, и она полностью подчинена RNC.

Общее описание стандарта TD-SCDMA.

Стандарт	TD-SCDMA
----------	----------

(TimeDivisionSynchronousCodeDivisionMultipleAccess) – множественный доступ с синхронным кодовым и временным разделением – это стандарт 3G, нашедший свое применение в Китае. Одной из причин разработки этого стандарта была попытка получить независимую от западного рынка сеть сотовой связи. Так же как и другие стандарты третьего поколения TD-SCDMA предоставляет расширенные возможности по передаче данных. Этот стандарт разрабатывался совместно компанией Siemens и Китайской академией технологий связи (CATT - China Academy of Telecommunications Technology). В марте 2001 года 3GPP (Third Generation Partnering Project) принял его как часть (метод доступа) четвертого выпуска стандарта UMTS.

Преимущества TD-SCDMA.

Основные отличия и преимущества стандарта TD-SCDMA перед другими стандартами сотовой связи:

— сеть хорошо подходит для асимметричного трафика 3G приложений, например, доступ в сеть Интернет. Приложения реального времени такие как голосовые соединения и мультимедиа, и они генерируют симметричный трафик. Для оффлайн приложений (e-mail, доступ в сеть Интернет) требования к задержкам меньше, а трафик обычно асимметричен, причем в направлении downlink (от BTS к MS) передается в несколько раз большие объемы данных. Для тех стандартов, которые требуют отдельных полос частот для uplink и downlink (GSM, CDMA2000, UMTS и т.п.) во время использования асимметричных приложений, занимаемые данные остаются не задействованными. Это в итоге приводит к уменьшению спектральной эффективности стандарта. В свою очередь, в стандарте TD-SCDMA данные в uplink и downlink передаются в одной полосе частот, что позволяет подобрать скорость полосы в точной необходимости с

требованиями приложений. Причем скорость может быть настроена достаточно точно, с небольшим шагом от 1,2 кбит/сек до 2Мбит/сек. Эти особенности позволяют более эффективно использовать имеющийся спектр частот;

— высокая спектральная эффективность приводит к увеличению емкости сети. Как отмечалось выше: в стандарте TD-SCDMA используется общая полоса на радио интерфейсе в uplink и downlink, что позволяет использовать все выделяемые ресурсы без остатка. Кроме того, благодаря другим технологиям (смарт-антенны, динамическое распределение ресурсов и т.п.) удастся снизить интерференцию в соте, и, соответственно, увеличить емкость сети (до 5 раз по сравнению с GSM). Это особенно важно в пригородных областях с плотной застройкой;

— увеличенная гибкость в использовании частотного ресурса и построении сети, которая обусловлена полосой пропускания 1,6 МГц.

К другим преимуществам TD-SCDMA можно отнести пониженное потребление мощности, экономия транспортных ресурсов, упрощенное планирование сети.

2.4 Четвертое поколение стандартов сотовой связи (4G)

LTE - Long Term Evolution (4G).

Стандарты третьего поколения позволяют предоставить широкий перечень мультимедийных услуг и поддерживают скорости передачи данных до 14Мбит/сек. Это вполне соответствует запросам абонентов в настоящее время. Однако, объемы передаваемой информации в телекоммуникационных сетях растут с каждым днем. Чтобы удовлетворить потребности пользователей по скорости передачи данных и набору услуг хотя бы на 20 лет вперед необходим новый стандарт, уже четвертого поколения.

Работа над первым стандартом четвертого поколения - LTE (Long Term Evolution) началась в 2004 году организацией 3GPP. Главными требованиями, которые предъявлялись в процессе работы над стандартом были следующие:

- скорость передачи данных выше 100 Мбит/сек;
- высокий уровень безопасности системы;
- высокая энергоэффективность;
- низкие задержки в работе системы;
- совместимость со стандартами второго и третьего поколений.

В конце 2009 года в Швеции была запущена в коммерческую эксплуатацию первая сеть стандарта LTE.

Сети LTE поддерживают скорости передачи данных до 326,4 Мбит/сек. К примеру, загрузка фильма в хорошем качестве займет менее одной минуты. Следовательно, верхняя планка по скорости передачи данных практически снимается. Структура сети стандарта LTE представлена на рисунке 8.

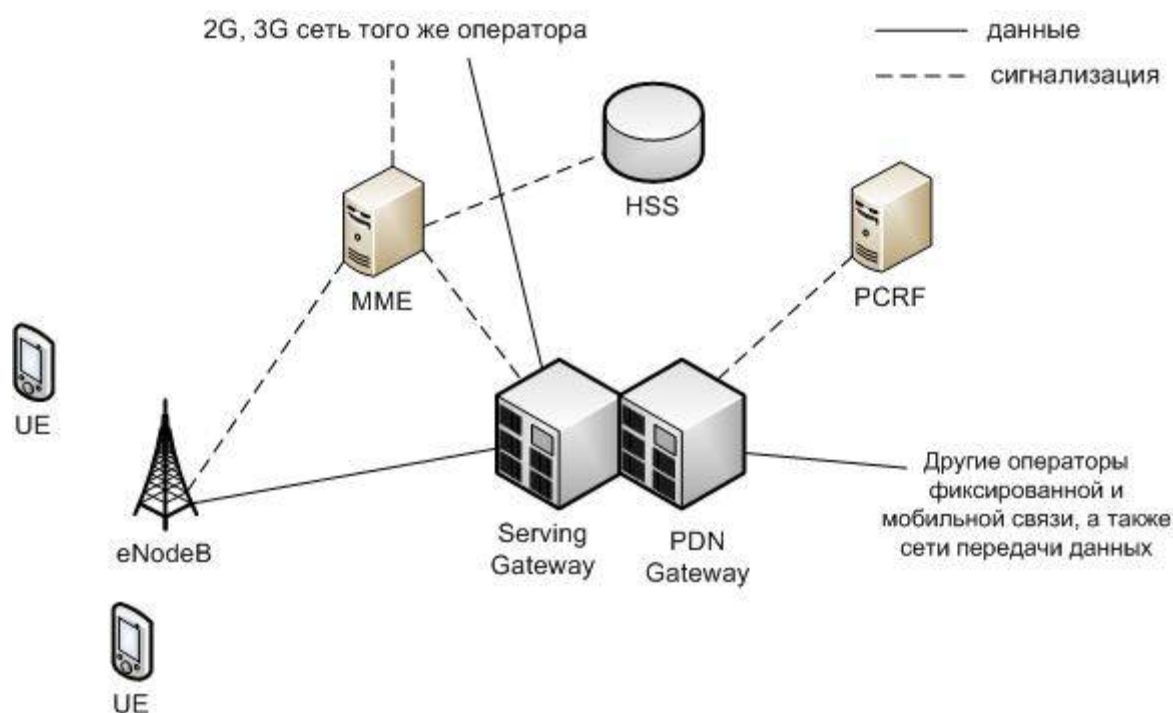


Рисунок 8 - Структура сети стандарта LTE

Из схемы сети LTE, представленной выше, уже видно, что структура сети сильно отличается от сетей стандартов 2G и 3G. Существенные изменения претерпела и подсистема базовых станций, и подсистема коммутации. Была изменена технология передачи данных между

оборудованием пользователя и базовой станцией. Также подверглись изменению и протоколы передачи данных между сетевыми элементами. Вся информация (голос, данные) передается в виде пакетов. Следовательно, уже нет разделения на части обрабатывающие либо только голосовую информацию, либо только пакетные данные.

Можно выделить следующие основные элементы сети стандарта LTE:

- обслуживающий шлюз сети LTE (Serving Gateway (SGW)). Предназначен для обработки и маршрутизации пакетных данных поступающих из/в подсистему базовых станций. По сути, заменяет MSC, MGW и SGSN сети UMTS. SGW имеет прямое соединение с сетями второго и третьего поколений того же оператора, что упрощает передачу соединения в /из них по причинам ухудшения зоны покрытия, перегрузок и т.п;
- шлюз к/от сетей других операторов (PDN Gateway (PGW)). Если информация (голос, данные) передаются из/в сети данного оператора, то они маршрутизируются именно через PGW;
- узелуправлениямобильностью (Mobility Management Entity (MME)). Предназначен для управления мобильностью абонентов сети LTE;
- сервер абонентских данных (HomeSubscriberServer (HSS)). HSS представляет собой объединение VLR, HLR, AUC выполненных в одном устройстве;
- узел выставления счетов абонентам за оказанные услуги связи (Policy and Charging Rules Function (PCRF)).

Все перечисленные выше элементы относятся к системе коммутации сети LTE. В системе базовых станций остался лишь один знакомый нам элемент – базовая станция, которая получила название eNodeB. Этот элемент выполняет функции и базовой станции, и контроллера базовых станций сети LTE. За счет этого упрощается расширение сети, т.к. не требуется расширение емкости контроллеров или добавления новых [5].

2.5 Пятое поколение стандартов сотовой связи (5G)

5G (от англ. fifth generation — «пятое поколение») — пятое поколение мобильной связи, действующее на основе стандартов телекоммуникаций, следующих за существующими стандартами 4G/IMT-Advanced[1]. Телекоммуникационный стандарт связи нового поколения.

Технологии 5G должны обеспечивать более высокую пропускную способность по сравнению с технологиями 4G, что позволит обеспечить бóльшую доступность широкополосной мобильной связи, а также использование режимов device-to-device (букв. «устройство к устройству», прямое соединение между абонентами), сверхнадёжные масштабные системы коммуникации между устройствами, а также меньшее время задержки, скорость интернета от 1 до 2 Гбит/с, меньший расход энергии батарей, чем у 4G-оборудования, что благоприятно скажется на развитии Интернета вещей.

Одной из ключевых технологий для реализации сетей сотовой связи 5G является использование в составе базовых станций многоэлементных цифровых антенных решёток с количеством антенных элементов 128, 256 и более. Соответствующие системы получили наименование Massive MIMO[5].

Для повышения спектральной эффективности, наряду с пространственным мультиплексированием, в 5G могут использоваться разновидности технологий неортогонального множественного доступа (NOMA) и N-OFDM-сигналов.

Для реализации системы важно на улице располагать передатчики на высоте выше двухэтажных автобусов. На практике это означает размещение аппаратуры на осветительных столбах, что привело даже к массовым судебным спорам (о цене и праве) в Великобритании.

Связь 5G использует два диапазона электромагнитных волн — FR1 (от 600 до 6000 МГц) и FR2 (от 24 до 100 ГГц) [5].

3 Рассмотрение источников утечки информации по каналам сотовой связи

3.1 Система технических средств для обеспечения функций оперативно-розыскных мероприятий

Во многих государствах мира операторы связи обязаны обеспечить доступ к линиям прослушивания телефонных каналов для уполномоченных органов. В России на практике это осуществляется технически путем использования СОРМ — системы технических средств для обеспечения функций оперативно-розыскных мероприятий. Каждый оператор связи обязан поставить на своей АТС интегрированный модуль СОРМ. Если оператор не установил у себя оборудование для прослушивания телефонов всех пользователей, его лицензия в России будет аннулирована. Аналогичные программы тотального прослушивания действуют в Белоруссии, Казахстане, на Украине, в США, Великобритании (Interception Modernisation Programme, Tempora) и других странах мира. Подавляющее число технических специалистов на самом деле имеет достаточно низкую квалификацию, что позволяет несанкционированно подключиться к системе незаметно для самих спецслужб.

Операторы связи не контролируют, когда и кого из абонентов слушают по линиям СОРМ, а также никак не проверяют, есть ли на прослушивание конкретного пользователя санкция суда [9].

3.2 Прослушивания через оператора

Операторы сотовой связи имеют возможность просматривать список звонков и историю перемещений мобильного телефона, который регистрируется в различных базовых станциях по своему физическому местоположению. Чтобы получить записи звонков, как у спецслужб, оператору нужно подключиться к системе СОРМ. По закону операторы обязаны хранить аудиозаписи разговоров всех пользователей от полугода до трёх лет [9].

3.3 Подключение к сигнальной сети SS7

С помощью уязвимости в протоколе сигнализации SS7 (Signaling System № 7) возможно прослушать телефон, подключившись к сети оператора сотовой сети. Специалисты по информационной безопасности описывают эту технику таким образом. Нарушитель внедряется в сеть SS7 и отправляет служебное сообщение Send Routing Info For SM (SRI4SM), указывая в качестве параметра телефонный номер атакуемого абонента А. В ответ на это домашняя сеть абонента А посылает атакующему некоторую техническую информацию: IMSI (международный идентификатор абонента) и адрес коммутатора MSC, который в настоящий момент обслуживает абонента. Далее нарушитель путем использования сообщения Insert Subscriber Data (ISD) внедряет в базу данных VLR обновлённый профиль абонента, меняя в нем адрес биллинговой системы на адрес своей, псевдобиллинговой, системы. Затем, когда жертва атаки совершает исходящий вызов, его коммутатор обращается вместо реальной биллинговой системы к системе атакующего, которая даёт коммутатору команду перенаправить вызов на третью сторону, подконтрольную нарушителю. На этой третьей стороне собирается конференц-вызов из трёх абонентов, два из которых реальные (вызывающий А и вызываемый В), а третий внедрён злоумышленником несанкционированно и может слушать и записывать разговор. Специалисты говорят, что при разработке сигнальной сети SS7 в ней не было спроектировано механизмов защиты от подобных атак. Подразумевалось, что эта система и так закрыта и защищена от подключения извне, но в реальности злоумышленник может найти способ подключиться к этой сигнальной сети. К сети SS7 можно подключиться в любой точке мира, например, в бедной азиатской или южноамериканской стране, — и вам будут доступны коммутаторы всех операторов в России, США, Европе и других странах. Данный метод дает возможность прослушать любого абонента в мире. Перехват входящих СМС

любого абонента тоже осуществляется элементарно, как и перевод баланса через USSD-запрос [9].

3.4 Поддельная базовая станция

Поддельная базовая станция имеет более сильный сигнал, чем настоящая БС. Соответственно она перехватывает трафик абонентов и позволяет использовать данные на телефоне. Известно, что фальшивые базовые станции широко используются правоохранными органами за рубежом. В США популярна модель фальшивой БС под названием StingRay. И не только правоохранные органы используют такие устройства. Например, предприниматели в Китае часто используют фальшивые базовые станции для массовой рассылки спама на мобильные телефоны, которые находятся в радиусе сотен метров вокруг. Вообще в Китае производство «фальшивых сот» осуществляется в промышленном масштабе, так что в местных магазинах не проблема отыскать данное устройство различных видов и ценового диапазона [9].

3.5 Фемтосоты

В последнее время в некоторых компаниях используются фемтосоты — маломощные небольшие станции сотовой связи, которые перехватывают трафик с сотовых телефонов, находящихся в радиусе действия. Такая фемтосота может записывать звонки всех сотрудников компании, прежде чем перенаправлять звонки на базовую станцию сотовых операторов. Следовательно, для прослушки абонента нужно поставить собственную фемтосоту или взломать оригинальную фемтосоту оператора.

3.6 Мобильный комплекс для дистанционного прослушивания каналов сотовой связи

В данном случае радиоантенна устанавливается недалеко от абонента (работает на расстоянии 500 метров). Направленная антенна, соединенная с компьютером, перехватывает все сигналы телефона, а по окончании работы её просто забирают в другое место. В отличие от фальшивой фемтосоты или трояна, здесь злоумышленнику не нужно думать о том, чтобы проникнуть на

место и установить фемтосоту, а потом убрать её (или удалить троян, не оставив следов проникновения). Возможностей современных компьютеров достаточно, чтобы записывать сигнал GSM на большом количестве частот, а затем расшифровать данные с помощью радужных таблиц. [6][9].

3.7 Устройства сотовой связи.

Для перехвата переговоров, ведущихся по мобильной сотовой связи необходимо применять сложную аппаратуру. В настоящее время существуют разные комплексы контроля сотовой системы связи стандартов AMPS, DAMPS, NAMPS, NMT-450, NMT-450i, разработанных и изготовленных в России и странах Западной Европы. Комплексы могут обнаруживать и сопровождать по частоте входящие и исходящие звонки абонентов сотовой связи, определять номера телефонов абонентов, производить слежение по частоте за каналом во время телефонного разговора, в том числе при передвижении из зоны покрытия одной соты в другую. Количество задаваемых для контроля абонентов определяется составом аппаратуры комплекса и версией программного обеспечения и может достигать до 16 и более.

Имеется возможность вести автоматическую запись переговоров на диктофон, вести на жестком диске ПЭВМ протокол записей на диктофон, производить полный мониторинг всех сообщений, передаваемых по служебному каналу, а также определять доступность всех базовых станций в точке их приема с ранжировкой по уровням принимаемых от базовых станций сигналов.

Стоимость подобных комплексов в зависимости от стандарта контролируемой системы связи и объемов решаемых задач может составлять от 1 до 60 тысяч долларов.

Ассоциация независимых разработчиков смарт-карт (Smartcard Developer Association) и двое исследователей из Университета Беркли сообщили, что им удалось клонировать сотовые телефоны стандарта GSM.

Стандарт GSM (Groupe Speciale Mobile), разработанный Европейским институтом телекоммуникационных стандартов (European Telecommunications Standard institute) является самым широко используемым в мире и применяется 79 млн. аппаратов мобильной связи, преимущественно в странах Европы и Азии. Ранее считалось, что телефоны GSM обладают настолько надежной защитой, что их нельзя не только прослушать, но и размножить, то есть сделать несколько аппаратов, одновременно пользующихся одним и тем же номером.

Преодоление защиты GSM еще раз показало, что единственная гарантия надежности криптографических алгоритмов - это их полная открытость. Засекреченные системы (использующиеся в GSM, и не только) практически неизбежно оказываются уязвимыми. Зашифрованные данные абонента GSM хранятся в небольшой смарт-карте, которая вставляется в телефон. Без карты, называемой также модулем идентификации пользователя (SIM - Subscriber Identification Module), телефон представляет собой бесполезную оболочку. Карту, идентифицирующую владельца, можно использовать с любым стандартным телефоном. Обнаруженная уязвимость в безопасности позволяет получить конфиденциальную информацию из одного SIM и записать ее в другой, создав точную копию первого телефона. Клонировать телефон, перехватывая информацию в эфире, пока нельзя, но SDA не исключает такой возможности в будущем. Установив, какие именно криптографические методы используются в GSM, SDA привлекла для их изучения двух исследователей из Университета Беркли - Дэвида Вагнера (David Vagner) и Айана Голдберга (Ian Goldberg). Менее чем за сутки они обнаружили слабость в алгоритме COMP128, который используется для защиты информации в SIM. По информации Вагнера, уязвимость давно бы нашли и устранили, если бы алгоритмы были опубликованы [6][9].

4 Выбор оборудования для исследования канала сотовой связи

Для обнаружения закладных устройств, работающих на частотах сотовой связи, используется следующий состав оборудования:

- SDR трансивер. С помощью данного устройства осуществляется сканирование радиоэфира для нахождения рабочих частот базовых станций операторов сотовой связи, перехват трафика, передающегося по найденным частотам;

- антенна;
- ПЭВМ.

Были определены следующие требования для выбора аппаратной части комплекса:

- SDR трансивер:
 - диапазон частот анализа сигналов от 100 кГц до 1,8 МГц;
 - поддержка всех основных видов модуляции;
 - чувствительность не менее 0,2 мВ;
 - полоса обзора от 250 кГц;
 - устойчивая работа в различных режимах применения;
- антенна:
 - диапазон частот от 30 кГц до 10 МГц;
 - ненаправленная;
 - малых охват сигнала;
- ПЭВМ:
 - двухъядерный процессор с тактовой частотой от 2 ГГц;
 - поддержка виртуализации;
 - ОЗУ 2 Гб;
 - 25 Гб свободного места на жёстком диске.

Для выбора SDR трансивера с целью включение в состав комплекса были рассмотрены следующие трансиверы:

- RTL-SDRR820T2. ;

- HackRFOne;
- BladeRF;
- USRP.

Сравнение основных характеристик рассмотренных SDR трансиверов, указано в таблице 1.

Таблица 1 - Основные характеристики моделей SDR трансиверов

Характеристики	Модель SDR трансивера			
	Realtek RTL2832U DVB-T	HackRF One	BladeRF	USRP
диапазон рабочих частот	100 кГц - 1,8 ГГц	1 МГц - 6 ГГц	300 МГц - 3,8 ГГц	70 МГц - 6 ГГц
модуляция	AM, FM, NFM, LSB, USB, CW	AM, FM, NFM, LSB, USB, CW	AM, FM, NFM, LSB, USB, CW	AM, FM, NFM, LSB, USB, CW
Частота дискретизации	2,8 МГц (может доходить до 3,2 МГц, но пропускает образцы)	до 20 МГц	до 20МГц	20МГц
экранированный корпус	нет	да	нет	да
стоимость, рублей	700	28000	35000	55000

При выборе SDR трансивера основными критериями будут являться:

- стоимость;

- диапазон частот;
- модуляция;
- частота выборки.

В ходе сравнительного анализа трансиверов, приведенных в таблице, было выявлено, что под необходимые условия подходят все варианты, поэтому итоговым фактором выбора стала стоимость оборудования. Необходимо выбрать SDR трансивер RTL-SDRR820T2. Общий вид RealtekRTL2832UDVB-T представлен на рисунках 9 и 10.



Рисунок 9 - Общий вид RealtekRTL2832UDVB-T

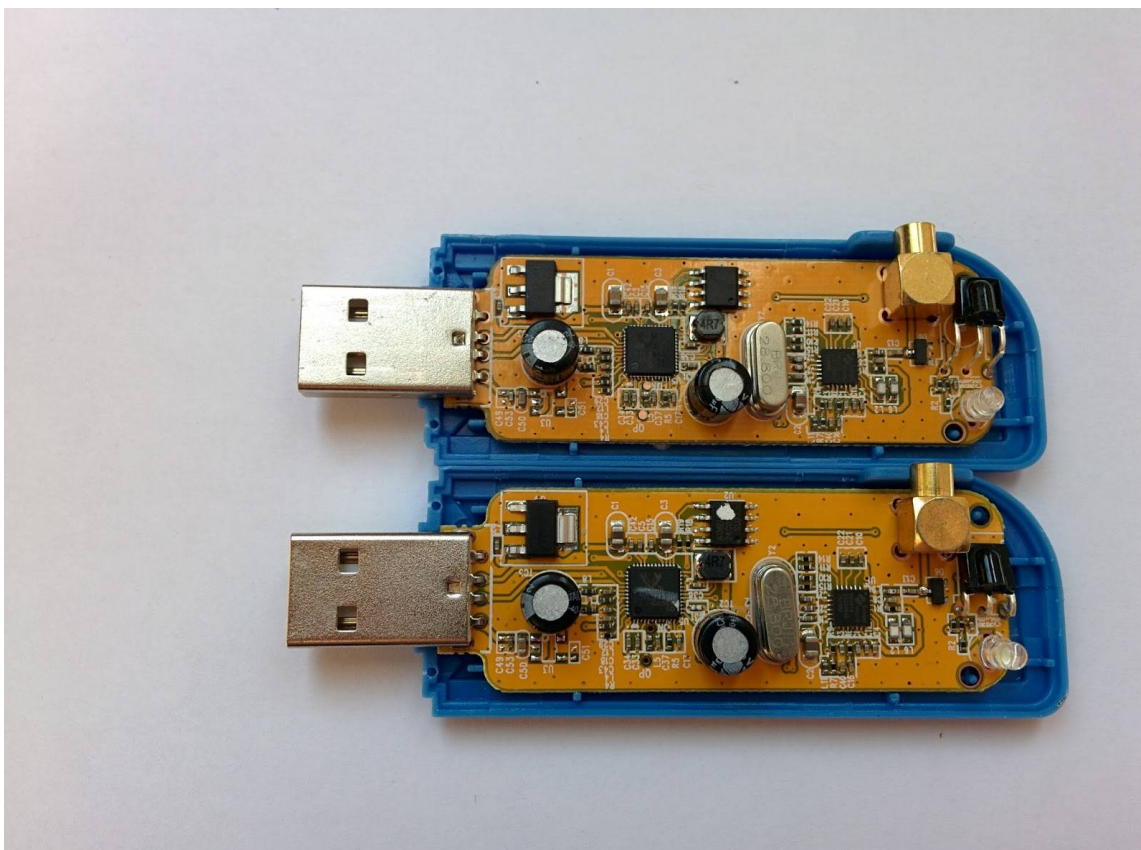


Рисунок 10 - Общий вид Realtek RTL2832UDVB-T без крышки
Основные характеристики Realtek RTL2832UDVB-T в таблице 2.

Таблица 2 - Основные характеристики Realtek RTL2832UDVB-T

Диапазон частот	100 кГц — 1750 МГц
Модуляция	AM, FM, NFM, LSB, USB, CW
Полоса обзора	меняется от 250 кГц до 3 МГц
Чувствительность	0.22 мКв (на 438 МГц в режиме NFM)
Входное сопротивление приёмника	50 Ом

Для целей применения данного комплекса не требуется антенна с большим радиусом покрытия, потому что более предпочтительна малая зона покрытия, чтобы выявлять закладные устройства в отдельно взятом помещении, не засоряя эфир отдалёнными объектами. Исходя из этого была взята стандартная антенна, входящая в комплект Realtek RTL2832UDVB-T [7]. Внешний вид антенна представлен на рисунке 11.



Рисунок 11 – Антенна из комплекта Realtek RTL2832U DVB-T
Системные требования для ПЭВМ:

- двухъядерный процессор от 2 ГГц (или лучше);
- ОЗУ 2 Гб;
- 25 Гб свободного места на жёстком диске;
- операционная система семейства Linux.

В качестве ПЭВМ был использован ноутбук Acer Extensa со следующими характеристиками:

- четырехъядерный процессор 1,6 ГГц;
- ОЗУ 4 Гб;
- 200 Гб свободного места на жёстком диске;
- операционная система Ubuntu 18.04 на базе среды виртуализации

VMware Workstation 15.

5 Определение требований к программному обеспечению комплекса

5.1 Общие требования к программному обеспечению комплекса для выявления закладных устройств, работающих на частотах сотовой связи

С помощью программного обеспечения выбирается частота, на которой работают ближайшие станции, а также сами закладные устройства, работающие на частотах сотовой связи, в связи с этим к нему предъявляются следующие требования:

- совместимость с аппаратными компонентами комплекса;
- наглядность представления информации;
- удобство пользовательского интерфейса;
- стабильное функционирование;
- возможность сохранения и фиксации результатов работы;
- широкий функционал и возможности применения;
- открытый исходный код;
- бесплатное распространение.

5.2 Требования к функционалу и возможностям программного обеспечения комплекса для выявления закладных устройств, работающих на частотах сотовой связи

Программное обеспечение должно выполнять следующие функции:

- возможность автоматического поиска рабочих частот базовых станций;
- возможность определения рабочих частот GSM;
- возможность перехвата и записи GSM-трафика;
- возможность декодирования GSM-трафика;

- возможность перехвата и декодирования GSM-трафика в режиме реального времени;
- возможность расширения функционала программного обеспечения комплекса для решения различных задач.

6 Выбор программного обеспечения комплекса

Для работы с SDR трансивером RealtekRTL2832UDVB-Тпонадобятся:

— GNU Radio — программный инструмент, предоставляющий разработчикам программно-определяемых радиосистем «строительные блоки», обеспечивающие основные функции цифровой обработки сигналов. Пользовательский интерфейс программы изображен на рисунке 12;

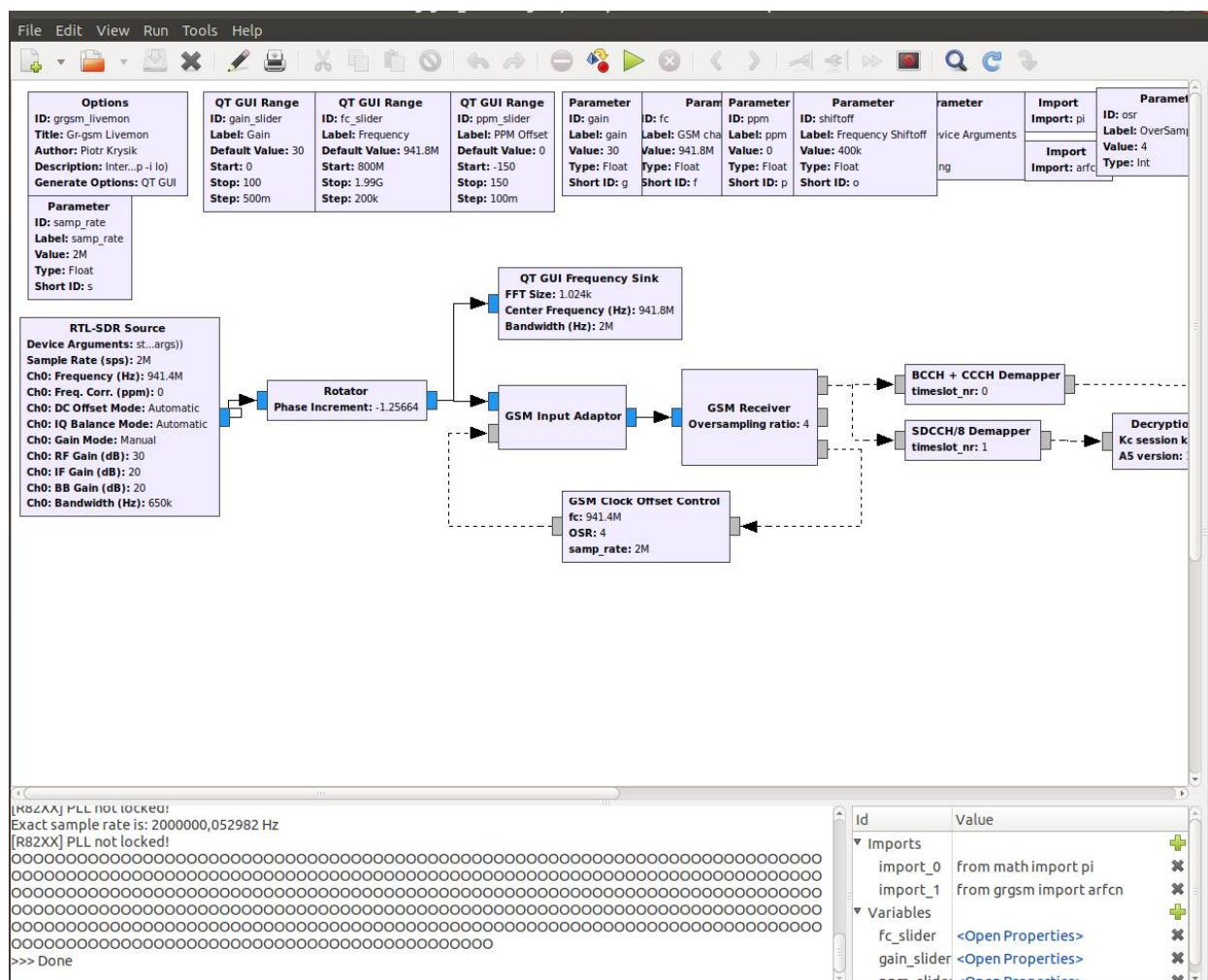


Рисунок 12 – Пользовательский интерфейс программы GNURadio

- GR-GSM – набор утилит для настройки GNURadio и перехвата GSM-трафика;

— Kalibrate-RTL - утилита для сканирования частот GSM. Демонстрирует частоты доступных каналов GSM, а также их смещения;

- Wireshark- программа-анализатор трафика для компьютерных сетей Ethernet и некоторых других. Имеет графический пользовательский

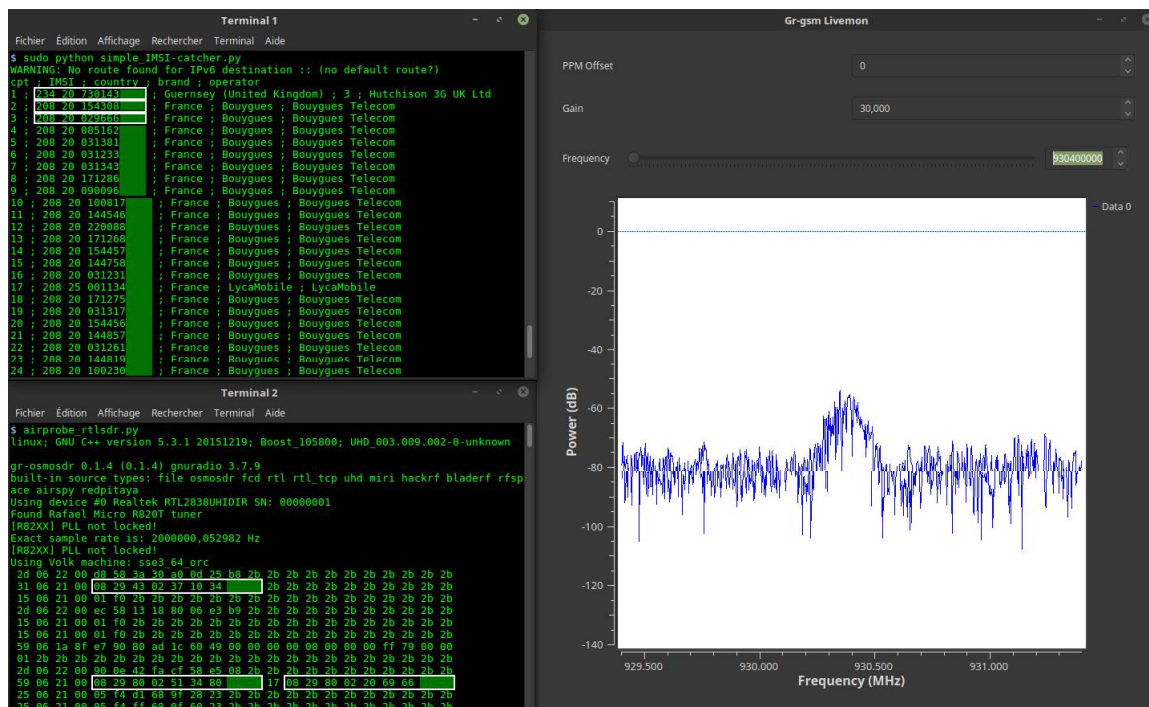
No.	Time	Source	Destination	Protocol	Length	Info
2695	622.58421906	127.0.0.1	127.0.0.1	GSMTAP	81 (CCCH) (SS)	
2696	622.61018406	127.0.0.1	127.0.0.1	GSMTAP	81 (CCCH) (RR)	Paging Request Type 3
2697	622.63018206	127.0.0.1	127.0.0.1	GSMTAP	81 (CCCH) (RR)	Paging Request Type 2
2698	622.65828006	127.0.0.1	127.0.0.1	GSMTAP	81 (CCCH) (RR)	Paging Request Type 2
2699	622.67631306	127.0.0.1	127.0.0.1	GSMTAP	81 (CCCH) (RR)	Paging Request Type 3
2700	622.70431106	127.0.0.1	127.0.0.1	GSMTAP	81 (CCCH) (RR)	Paging Request Type 1
2701	622.72117606	127.0.0.1	127.0.0.1	GSMTAP	81 (CCCH) (RR)	Paging Request Type 2
2702	622.75036606	127.0.0.1	127.0.0.1	GSMTAP	81 (CCCH) (RR)	Paging Request Type 3
2703	622.76742306	127.0.0.1	127.0.0.1	GSMTAP	81 (CCCH) (RR)	Paging Request Type 3
2704	622.80014906	127.0.0.1	127.0.0.1	GSMTAP	81 (CCCH) (RR)	System Information Type 4 [Malformed Packet]
2705	622.81953806	127.0.0.1	127.0.0.1	GSMTAP	81 (CCCH) (SS)	
2706	622.84608506	127.0.0.1	127.0.0.1	GSMTAP	81 (CCCH) (RR)	Paging Request Type 2

▶Frame 2698: 81 bytes on wire (648 bits), 81 bytes captured (648 bits) on interface 0
 ▶Ethernet II, Src: 00:00:00:00:00:00 (00:00:00:00:00:00), Dst: 00:00:00:00:00:00 (00:00:00:00:00:00)
 ▶Internet Protocol Version 4, Src: 127.0.0.1 (127.0.0.1), Dst: 127.0.0.1 (127.0.0.1)
 ▶User Datagram Protocol, Src Port: 48217 (48217), Dst Port: 4729 (4729)
 ▶GSM TAP Header, ARFCN: 549 (Downlink), TS: 0, Channel: PCH (0)

```

0000  00 00 00 00 00 00 00 00 00 00 00 08 00 45 00  .....E.
0010  00 43 a1 47 40 00 40 11 9b 60 7f 00 01 7f 00  .C.G@.@.
0020  00 01 bc 59 12 79 00 2f fe 42 02 04 01 00 02 25  ...Y.y./ .B.....%
0030  b6 00 00 05 bb b8 05 00 00 49 06 22 00 79 5b  .....".I..y|
0040  f8 28 7d 53 dh 50 17 a5 fd cd 31 38 d1 8a 2b 2b  /3S p      18 ++
  
```

— IMSI-catcher - Python-скрипт, который обрабатывает данные из gr-gsm и извлекает номера IMSI. Пользовательский интерфейс программы изображен на рисунке 14.



45

7 Описание поиска информативного сигнала по каналам сотовой связи

Существует несколько способов поиска информативного сигнала по каналам сотовой связи с помощью SDR трансивера RealtekRTL2832UDVB-T:

- ручное сканирование частот с помощью GR-GSM. Для этого необходимо выполнить следующие действия:

- открыть терминал командной строки;
- запустить утилиту `grgsm_livemon` из пакета GNURadio;
- с помощью перебора частот в диапазоне от 900 до 1800

МГц произвести поиск информативного сигнала GSM. При нахождении рабочих частот GSMсотовых операторов связи в командной строке начнут отображаться байты данных, как показано на рисунке 15;

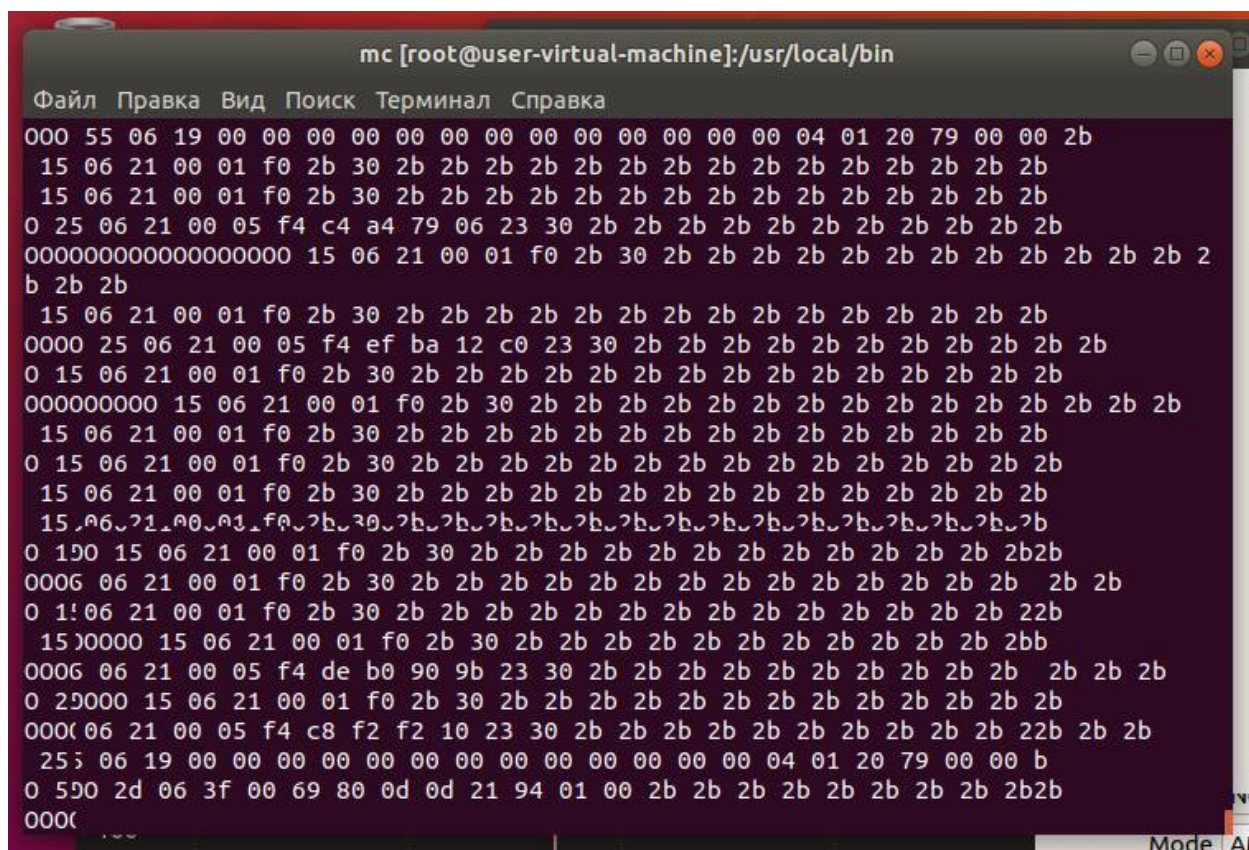
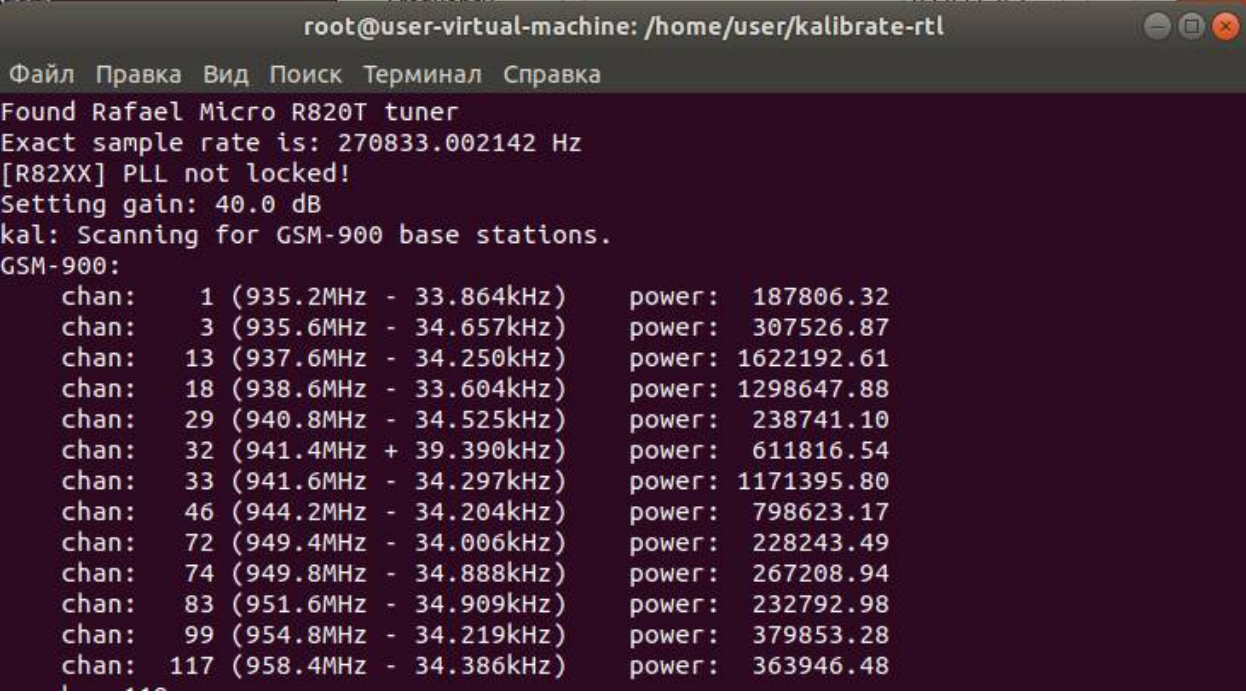


Рисунок 15 – Байты данных пакетов GSM

- сканирование частот с помощью утилиты Kalibrate-RTL. Для этого необходимо выполнить следующие действия:

- открыть терминал командной строки;

— запустить утилиту `Kalibrate-RTL` путем использования команды `kal -s 900 -g 40`. Через несколько минут на экране появятся доступные каналы GSM операторов сотовой связи с указанием рабочей частоты, её смещения и амплитуды. Результат выполнения изображен на рисунке 16;



```
root@user-virtual-machine: /home/user/kalibrate-rtl
Файл Правка Вид Поиск Терминал Справка
Found Rafael Micro R820T tuner
Exact sample rate is: 270833.002142 Hz
[R82XX] PLL not locked!
Setting gain: 40.0 dB
kal: Scanning for GSM-900 base stations.
GSM-900:
chan: 1 (935.2MHz - 33.864kHz) power: 187806.32
chan: 3 (935.6MHz - 34.657kHz) power: 307526.87
chan: 13 (937.6MHz - 34.250kHz) power: 1622192.61
chan: 18 (938.6MHz - 33.604kHz) power: 1298647.88
chan: 29 (940.8MHz - 34.525kHz) power: 238741.10
chan: 32 (941.4MHz + 39.390kHz) power: 611816.54
chan: 33 (941.6MHz - 34.297kHz) power: 1171395.80
chan: 46 (944.2MHz - 34.204kHz) power: 798623.17
chan: 72 (949.4MHz - 34.006kHz) power: 228243.49
chan: 74 (949.8MHz - 34.888kHz) power: 267208.94
chan: 83 (951.6MHz - 34.909kHz) power: 232792.98
chan: 99 (954.8MHz - 34.219kHz) power: 379853.28
chan: 117 (958.4MHz - 34.386kHz) power: 363946.48
```

Рисунок 16 – Каналы GSM с указанием рабочей частоты, её смещения и амплитуды

— сканирование частот с помощью утилиты `grgsm_scanner`. Для этого необходимо выполнить следующие действия:

- открыть терминал командной строки;
- запустить утилиту `grgsm_scanner` путем использования команды `grgsm_scanner`. Через несколько минут на экране появятся доступные каналы GSM операторов сотовой связи с указанием ARFCN, рабочей частоты, ID оператора, уровня сигнала от ближайшей БС. Результат выполнения изображен на рисунке 17.

```
mc [user@user-virtual-machine]:/usr/local/bin
Файл Правка Вид Поиск Терминал Справка
user@user-virtual-machine:~$ mc
user@user-virtual-machine:/usr/local/bin$ ./grgsm_scanner
linux; GNU C++ version 7.3.0; Boost_106501; UHD_003.010.003.000-0-unknown

ARFCN: 1, Freq: 935.2M, CID: 0, LAC: 56800, MCC: 250, MNC: 1, Pwr: -43
ARFCN: 3, Freq: 935.6M, CID: 121, LAC: 56800, MCC: 250, MNC: 1, Pwr: -40
ARFCN: 8, Freq: 936.6M, CID: 0, LAC: 56800, MCC: 250, MNC: 1, Pwr: -45
ARFCN: 29, Freq: 940.8M, CID: 0, LAC: 0, MCC: 0, MNC: 0, Pwr: -46
ARFCN: 47, Freq: 944.4M, CID: 0, LAC: 0, MCC: 0, MNC: 0, Pwr: -41
ARFCN: 50, Freq: 945.0M, CID: 46426, LAC: 56165, MCC: 250, MNC: 99, Pwr: -43
ARFCN: 56, Freq: 946.2M, CID: 0, LAC: 0, MCC: 0, MNC: 0, Pwr: -34
ARFCN: 83, Freq: 951.6M, CID: 0, LAC: 0, MCC: 0, MNC: 0, Pwr: -44

user@user-virtual-machine:/usr/local/bin$
```

Рисунок 17 – Сканирование частот GSM с помощью утилиты grgsm_scanner с указанием ARFCN, рабочей частоты, ID оператора, уровня сигнала от ближайшей БС

8 Структура разработанного комплекса, предназначенного для выявления закладных устройств, работающих на частотах сотовой связи

Собранный комплекс для обнаружения закладных устройств, работающих на частотах сотовой связи состоит из следующего оборудования:

- ПЭВМ;
- SDR трансивер RealtekRTL2832UDVB-T;
- антенна стандартная из комплекта SDR трансивера.

Структура комплекса для выявления акустоэлектрических закладных устройств, представлена на рисунке 18.

SDR трансивер RealtekRTL2832UDVB-T подключается к ПЭВМ по интерфейсу USB 2.0. Антенна коаксиальным кабелем из комплекта SDR трансивера подключается к входному разъёму типа BNC и осуществляет приём сигнала GSM. На ПЭВМ было установлено специализированное программное обеспечение для сопряжения SDR трансивера с ПЭВМ. Так же, с помощью программного обеспечения осуществляется поиск рабочих частот GSM, определение каналов базовых станций операторов сотовой связи, а также декодирование данных GSM.

SDR трансивер Realtek RTL2832U
RTL-SDR DVB-T



Рисунок 18 – Структура комплекса для выявления закладных устройств, работающих на частотах сотовой связи

9 Разработка методических рекомендаций по выявлению закладных устройств, работающих на частотах сотовой связи и руководства пользователя разработанного комплекса

9.1 Регламент применения комплекса для выявления закладных устройств, работающих на частотах сотовой связи

Общие положения.

Требования настоящего регламента распространяются на все сферы применения комплекса для выявления закладных устройств (далее комплекс), работающих на частотах сотовой связи, включая проведение специальных проверок и других видов работ с его использованием. Целью разработки настоящего регламента является реализация оптимизации работы специалистов по защите информации, минимизация ошибок и предупреждение правонарушений, связанных с использованием данного комплекса.

Назначение.

Настоящий Регламент определяет порядок использования комплекса для выявления закладных устройств, работающих на частотах сотовой связи.

Область применения.

Требования и правила настоящего Регламента распространяются на все категории работников, осуществляющие применение данного комплекса. Настоящий регламент описывает этапы проведения поиска закладных устройств, работающих на частотах сотовой связи.

Нормативные ссылки.

Регламент разработан на основании:

— Постановления Правительства РФ от 16.04.2012 N 314 "Об утверждении Положения о лицензировании деятельности по выявлению электронных устройств, предназначенных для негласного получения информации (за исключением случая, если указанная деятельность осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)" [2];

— ГОСТ Р 50922-2006 Защита информации. Основные термины и определения [1];

— УК РФ Статья 138. Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений [14].

Ответственность.

Работники организации, осуществляющей применение данного комплекса, несут дисциплинарную, административную и уголовную ответственность за ненадлежащее использование или неисполнение требований настоящего Регламента.

За несанкционированное или нецелевое применение комплекса, повлекшее за собой правонарушение предусмотрена наказание по статье 138 УК РФ.

Работники, отвечают за:

- применение комплекса;
- работоспособность комплекса;
- хранение комплекса.

Требования, предъявляемые к работникам, осуществляющим применение данного комплекса:

- наличие профильного образования в области информационной безопасности, либо прохождения курсов повышения квалификации;
- навыки проведения специальных проверок объектов информатизации.

Контроль использования осуществляет начальник подразделения по информационной безопасности организации, либо её руководитель.

Методические рекомендации.

Технология обнаружения закладных основана на анализе сигналов ближайших базовых станций и их взаимодействии абонентами.

При подготовке к проведению измерений необходимо:

- убедиться в отсутствии функционирующих устройств зашумления радиосигналов, находящихся рядом;
- проверить наличие сигналов от базовых станций операторов сотовой связи;
- убедиться в отсутствии устройств сотовой связи поблизости.

Проверку помещения на наличие закладных устройств, работающих по каналам сотовой связи необходимо проводить без изменения расположения находящихся в нем предметов и технических средств. Комплекс рекомендуется располагать ближе к центру исследуемого помещения.

9.2 Порядок проведения проверки помещения на наличие закладных устройств, работающих на частотах сотовой связи

Порядок проведение проверки:

- производиться осмотр помещения и определение находящихся в нем технических средств, возможных мест установки закладных устройств и других замаскированных средств негласного получения информации;
- проверить работоспособность аппаратных компонентов комплекса путем тестового включения;
- проверить работоспособность программного обеспечения комплекса путем запуска. В случае необходимости установить актуальные обновления;
- подключить SDR трансивер к ПЭВМ и произвести измерения;
- проанализировать полученную информацию о сигналах базовых станций и выявить ближайшие из них;
- проанализировать полученную информацию о сигналах ближайших устройств, работающих на частотах сотовой связи и определить их идентификаторы;

— на основании полученных данных определить меры по проведению организационных мер по изъятию закладных устройств и других несанкционированных устройств негласного получения информации;

— на основании полученных данных определить технические меры защиты конфиденциальной информации [11].

9.3 Руководство пользователя комплекса для выявления закладных устройств, работающих на частотах сотовой связи

Введение.

Обнаружение закладочных устройств, как и любых других объектов, осуществляется по их демаскирующим признакам. Демаскирующие признаки закладных устройств — объективно существующие и устойчиво повторяющиеся признаки функционирования или физического присутствия объекта позволяющие обнаружить, распознать объект и получить другую необходимую информацию о нём. Вероятность обнаружения объекта тем выше, чем больше демаскирующих признаков и чем они информативнее в признаковой структуре. Одним из видов демаскирующих признаков являются сигнальные признаки. Сигнальными признаками ЗУ является вид, моменты появления и параметры излучаемого ими сигнала.

Поиск по сигнальным признакам осуществляется с помощью специальных технических средств, способных визуализировать или представить излучаемый закладкой сигнал в другом, удобном для анализа, виде. К таким техническим средствам относится данный комплекс [10].

Область применения.

Комплекс предназначен для выявления закладных устройств, работающих на частотах сотовой связи путем определения их рабочих частот и идентификаторов устройств.

Краткое описание возможностей.

Данный комплекс имеет следующие возможности:

- осуществлять ручной поиск в частотном диапазоне GSM850, GSM900, GSM1800;
- осуществлять автоматический поиск рабочих частот ближайших базовых станций операторов сотовой связи;
- осуществлять перехват данных GSM;
- осуществлять декодирование данных GSM-пакетов;
- осуществлять фильтрацию данных декодированных GSM-пакетов по различным параметрам и выявлять идентификаторы устройств.

Уровень подготовки пользователя:

- наличие навыков работы и администрирования операционных систем LinuxUbuntu 18.04;
- наличие профильного образования в области информационной безопасности или прохождения курсов повышения квалификации.

Перечень эксплуатационных документов, с которым необходимо ознакомиться:

- Руководство пользователяLinuxUbuntu 18.04;
- Регламент применения комплекса для выявления закладных устройств, работающих на частотах сотовой связи.

Назначение и условия применения.

Комплекс предназначен для выявления закладных устройств, работающих на частотах связи.

При подготовке к проведению измерений необходимо:

- убедиться в отсутствии функционирующих устройств зашумления радиосигналов, находящихся рядом;
- проверить наличие сигналов от базовых станций операторов сотовой связи;
- убедиться в отсутствии устройств сотовой связи поблизости.

Проверку помещения на наличие закладных устройств, работающих по каналам сотовой связи необходимо проводить без изменения расположения

находящихся в нем предметов и технических средств. Комплекс рекомендуется располагать ближе к центру исследуемого помещения

Системные требования к ПЭВМ, входящих в состав комплекса:

- двухъядерный процессор от 2 ГГц (или лучше);
- ОЗУ 2 Гб или больше;
- не менее 25 Гб свободного места на жёстком диске;
- операционная система семейства версии не ниже LinuxUbuntu

18.04.

Для подготовки к работе необходимо установить GNURadios набором утилит GR-GSM.

Для установкиGNURadios набором утилит GR-GSM необходимо выполнить в терминале командной строки следующие действия:

- установить необходимыеdev-пакеты командой
`sudoaptinstallgnuradiognuradio-devgitcmakeautoconflibtoolpkg-configg++ gccmakelibc6 \`
`libc6-devlibcppunit-1.14-0 libcppunit-devswigdoxygenliblog4cpp5v5 liblog4cpp5-devpython-scipy \`
`gr-osmosdr libosmocore libosmocore-dev;`

- выполнить сборку и установку проекта с помощью команд:

- `git clone https://git.osmocom.org/gr-gsm;`
- `cd gr-gsm;`
- `mkdir build;`
- `cd build;`
- `cmake .. ;`
- `make;`
- `sudomakeinstall;`

- выполнить конфигурирование системы командой
`sudoldconfig;`

- установить утилитуIMSI-catcher командами:

```

— sudo apt install python-numpy python-scipy
python-scapy;
— git clone https://github.com/Oros42/IMSI-
catcher.git;
— установить программу Wireshark командой sudo apt install
wireshark;
— установить программу GQRX командой
sudo apt install gqr;
— установить утилиту kalibrate-rtl командами:
— sudo apt install build-essential libtool
automake autoconf librtlsdr-dev libfftw3-dev;
— git clone https://github.com/steve-
m/kalibrate-rtl;
— cd kalibrate-rtl;
— ./bootstrap && CXXFLAGS='-W -Wall -O3';
— ./configure;
— make;
— sudo make install.

```

После установки программного обеспечения необходимо подключить SDR трансивер с антенной в разъём USB 2.0. Не рекомендуется подключать к разъёму USB 3.0 по причине возможных помех.

Инструкция по использованию программного обеспечения:

```

— запустить утилиту grgsm_scanner для поиска сигналов
ближайших базовых станций операторов сотовой связи с помощью команды
grgsm_scanner. Через минуту на экране появятся доступные каналы GSM
операторов сотовой связи с указанием ARFCN, рабочей частоты, ID
оператора, уровня сигнала от ближайшей БС. Результат выполнения
изображен на рисунке 19. Также каналы операторов сотовой связи можно

```

получить с помощью утилиты kalibrate-rtl с использованием команды `kal -s 900 -g 40`. Через несколько минут на экране появятся доступные каналы GSM операторов сотовой связи с указанием рабочей частоты, её смещения и амплитуды. Результат выполнения изображен на рисунке 20;

```
mc [user@user-virtual-machine]:/usr/local/bin
Файл Правка Вид Поиск Терминал Справка
user@user-virtual-machine:~$ mc
user@user-virtual-machine:/usr/local/bin$ ./grgsm_scanner
linux; GNU C++ version 7.3.0; Boost_106501; UHD_003.010.003.000-0-unknown

ARFCN: 1, Freq: 935.2M, CID: 0, LAC: 56800, MCC: 250, MNC: 1, Pwr: -43
ARFCN: 3, Freq: 935.6M, CID: 121, LAC: 56800, MCC: 250, MNC: 1, Pwr: -40
ARFCN: 8, Freq: 936.6M, CID: 0, LAC: 56800, MCC: 250, MNC: 1, Pwr: -45
ARFCN: 29, Freq: 940.8M, CID: 0, LAC: 0, MCC: 0, MNC: 0, Pwr: -46
ARFCN: 47, Freq: 944.4M, CID: 0, LAC: 0, MCC: 0, MNC: 0, Pwr: -41
ARFCN: 50, Freq: 945.0M, CID: 46426, LAC: 56165, MCC: 250, MNC: 99, Pwr: -43
ARFCN: 56, Freq: 946.2M, CID: 0, LAC: 0, MCC: 0, MNC: 0, Pwr: -34
ARFCN: 83, Freq: 951.6M, CID: 0, LAC: 0, MCC: 0, MNC: 0, Pwr: -44

user@user-virtual-machine:/usr/local/bin$
```

Рисунок 19– Сканирование частот GSM с помощью утилиты grgsm_scanner с указанием ARFCN, рабочей частоты, ID оператора, уровня сигнала от ближайшей БС

```
root@user-virtual-machine: /home/user/kalibrate-rtl
Файл Правка Вид Поиск Терминал Справка
Found Rafael Micro R820T tuner
Exact sample rate is: 270833.002142 Hz
[R82XX] PLL not locked!
Setting gain: 40.0 dB
kal: Scanning for GSM-900 base stations.
GSM-900:
chan: 1 (935.2MHz - 33.864kHz) power: 187806.32
chan: 3 (935.6MHz - 34.657kHz) power: 307526.87
chan: 13 (937.6MHz - 34.250kHz) power: 1622192.61
chan: 18 (938.6MHz - 33.604kHz) power: 1298647.88
chan: 29 (940.8MHz - 34.525kHz) power: 238741.10
chan: 32 (941.4MHz + 39.390kHz) power: 611816.54
chan: 33 (941.6MHz - 34.297kHz) power: 1171395.80
chan: 46 (944.2MHz - 34.204kHz) power: 798623.17
chan: 72 (949.4MHz - 34.006kHz) power: 228243.49
chan: 74 (949.8MHz - 34.888kHz) power: 267208.94
chan: 83 (951.6MHz - 34.909kHz) power: 232792.98
chan: 99 (954.8MHz - 34.219kHz) power: 379853.28
chan: 117 (958.4MHz - 34.386kHz) power: 363946.48
```

Рисунок 20– Каналы GSMс указанием рабочей частоты, её смещения и амплитуды

- выбрать частоты с самым сильным сигналом и запускать утилиту `grgsm_livemon` командой `grgsm_livemon`;
- установить найденную частоту в `grgsm_livemon` и найти поток байтов данных GSM, как показано на рисунках 21 и 22;

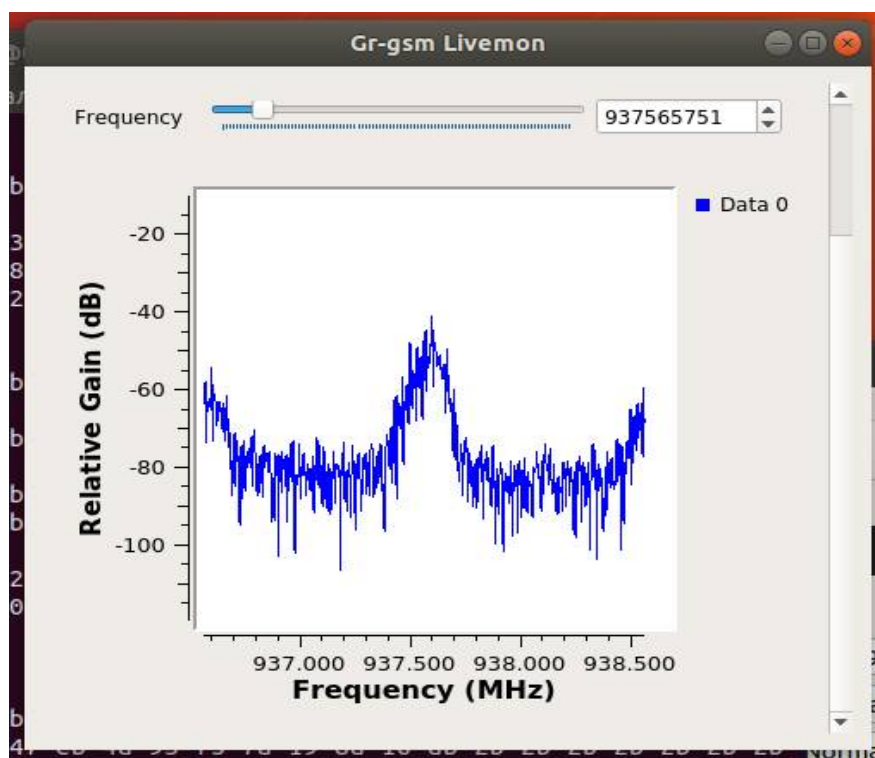


Рисунок 21– Выставление частоты в `grgsm_livemon`

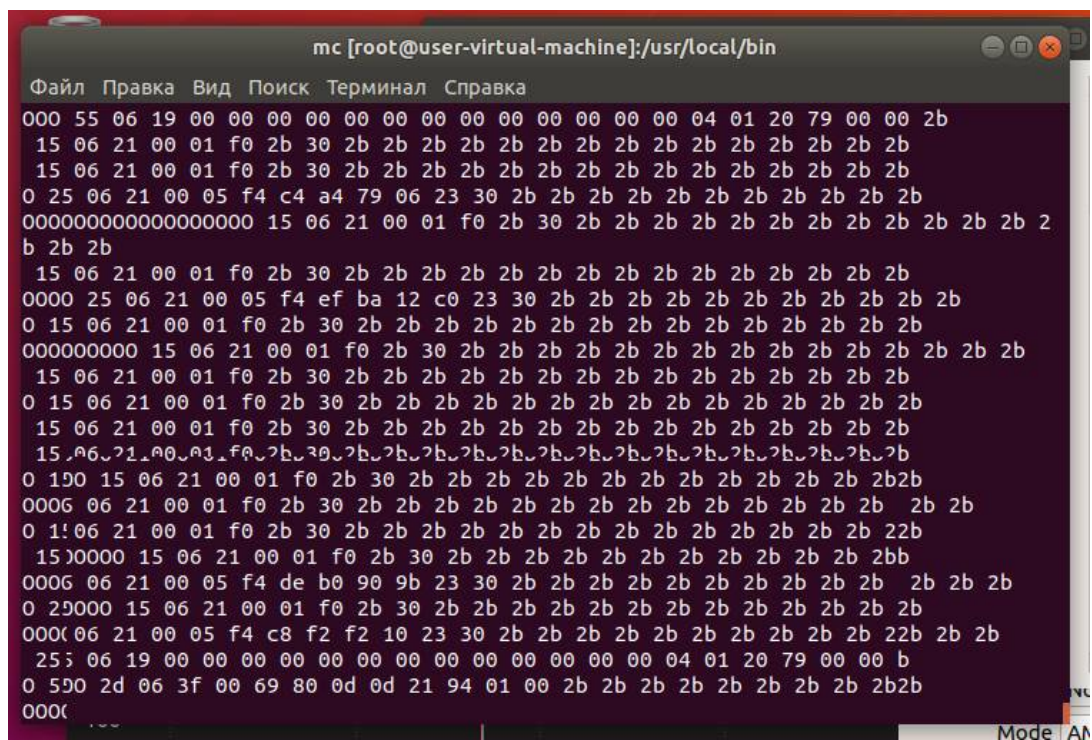


Рисунок 22– Байты данных, передающиеся по каналу GSM

— запустить программу Wireshark с использованием фильтра e212.imsi утилиты IMSI-cather с помощью команды `sudo wireshark -k -f udp -Ye212.imsi -ilo`.

В результате можно будет получить отфильтрованный список декодированных пакетов с указанием IMSI-идентификаторов ближайших устройств.

Проверка работоспособности системы.

Программное обеспечение работоспособно, если в результате действий пользователя, изложенных в п.п.3.1, корректно выполнены описанные операции и не было выведено сообщений об ошибках в виде сообщений командной строки.

Описание операций.

При ошибках в работе аппаратных средств восстановление функции системы возлагается на ОС.

При ошибках, связанных с программным обеспечением (ОС и драйверы устройств), восстановление работоспособности возлагается на ОС.

При неверных действиях пользователей, неверных форматах или недопустимых значениях входных данных, система выдает пользователю соответствующие сообщения, после чего возвращается в рабочее состояние, предшествовавшее неверной (недопустимой) команде или некорректному вводу данных.

Рекомендации по освоению.

Для успешного применения данного комплекса необходимо иметь навыки работы с ПК и изучить следующее:

- руководство пользователя Linux Ubuntu 18.04;
- регламент применения комплекса для выявления закладных устройств, работающих на частотах сотовой связи;
- описание основных стандартов сотовой связи;
- настоящее «Руководство пользователя» [12].

10 Вредные психофизические факторы, влияющие на органы зрения специалиста по защите информации. Методы и средства физической культуры, снижающие их воздействие

Специалист по защите информации во время выполнения своих трудовых обязанностей подвергается вредным факторам на производстве.

Профессиональная деятельность специалистов по защите информации состоит, как правило, из сведений ограниченного доступа и обработкой огромного объема информации, непосредственного контакта и консультирование с людьми, выполнения работы в сжатые рабочие сроки. Все эти факторы усиливают информационную нагрузку, что обуславливаются наличием нагрузки на органы зрения специалиста по защите информации. Под информационной нагрузкой понимается восприятие системами организма информации, которая оказывает влияние на органы зрения и способна вызвать негативные последствия для специалиста по информационной безопасности. Работа в течение долгого времени за персональной электронной вычислительной машине (ПЭВМ) способствует появлению усталости и напряжения органов зрения. На специалиста по защите информации, который работает на ПЭВМ могут действовать следующие вредные факторы:

- загрязнение воздуха вредными веществами, пылью, микроорганизмами;
- несоответствие нормам параметров микроклимата;
- повышенный уровень шума на рабочем месте;
- повышенный уровень статистического электричества при неправильно спроектированной рабочей зоне;
- широкий спектр излучения от дисплея, который включает рентгеновскую, ультрафиолетовую и инфракрасную области, а также широкий диапазон электромагнитных излучений других частот;

- повышенный уровень электромагнитных излучений;
- отсутствие или недостаток естественного света;
- недостаточная освещенность рабочей зоны;
- повышенная яркость света;
- повышенная пульсация светового потока (мерцание изображения);

- длительное пребывание в одном и том же положении и повторение одних и тех же движений приводит к синдрому длительных статических нагрузок (СДСН) [15];

- нерациональная организация рабочего места;
- умственное перенапряжение, которое обусловлено характером решаемых задач приводит к синдрому длительных психологических нагрузок (СДПН).

При работе на ПЭВМ органы зрения специалиста по защите информации выдерживают большую нагрузку, что может приводить центральной нервной системы. Так же повышенная сосредоточенность на выполнение ответственного задания, которое возложено на специалистов по защите информации, довольно часто приводит к огромным нагрузкам, способствует появлению боли и раздражения органов зрения [15].

За последние годы у специалистов по защите информации отмечаются жалобы общевегетативного характера такие как [15]:

- утомляемость;
- головные боли;
- тяжесть в голове;
- плохой сон;
- снижение бодрости;
- снижение работоспособности.

Длительный дискомфорт в условиях малой физической активности и способствует развитию заболеваний органов зрения.

Существует огромное количество методов для укрепления органов зрительной системы. В можно выделить следующие советы и рекомендации, при которых соблюдается гигиена зрения:

- необходимо обустроить собственное рабочее место правильным образом. Если речь идет о работе с компьютером, необходимо, обеспечить хорошее освещение, которое будет ярче экрана. Кроме того, расстояние от экрана до глаз не должно быть менее 50 см. Монитор или книга должны находиться на уровне несколько ниже глаз. Кроме того, не рекомендуется читать лежа и особенно;

- важно делать перерывы. Во время работы следует делать перерывы на 3-5 минут. Особенно такие перерывы важны при выполнении мелкой работы, требующей высокой концентрации внимания. Во время перерыва следует переводить взгляд на удаленный объект, тем самым изменять фокусировку взгляда. Период работы за компьютером может составить 1,5-2 часа;

- необходимо устраивать физкультурные паузы. Для этого рекомендуется передвигать глаза в стороны и по диагонали. Зрение нужно сфокусировать на близком предмете, а затем переводить взгляд вдаль. В промежутке нескольких секунд рекомендуется часто поморгать глазами и придержать наружные уголки;

- выполнять массаж. При первых признаках утомления стоит сделать массаж. Для этого необходимо прикрыть веки теплыми ладонями и слегка погладить, а затем, надавить на глаза;

- необходимо хотя бы раз в день устраивать глазам душ. Для этого нужно набрать в руки воду и глазами в ней поморгать;

- важно правильно питаться, а именно, включить в меню нужное количество зелени, овощей, желто-оранжевых фруктов, растительного масла, орехов и рыбы. Из напитков, следует отдать предпочтение зеленому чаю;

— необходимо защищать глаза от ультрафиолета. Важно носить в летние месяцы стеклянные очки с надежным фильтром. Категорически не рекомендуется носить очки с затемненными линзами, но без фильтра;

— рекомендуется бросить курить, потому что сигаретный дым очень вреден для зрения.

Соблюдая эти простые советы и рекомендации, специалисты по защите информации могут защитить глаза от вредного воздействия и различных заболеваний.

Заключение

В результате выполнения ВКР был разработан комплекс, предназначенный для выявления закладных устройств, работающих по каналам сотовой связи.

В процессе выполнения дипломного проекта была проанализирована существующая нормативно - правовая база в области защиты информации, рассмотрены основные стандарты сотовой связи и технические каналы утечки информации. Был осуществлен выбор оборудования, определение требований и выбор программного обеспечения комплекса для выявления закладных устройств, работающих по каналам сотовой связи. Была описана структура разработанного комплекса.

На заключительном этапе были разработаны методические рекомендации по выявлению для выявления закладных устройств, работающих на частотах сотовой связи и руководство пользователя.

Данный комплекс может быть использован в учебном процессе по дисциплине ТЗИ.

Протокол проверки ВКР на оригинальность приведен в Приложение А на рисунке А.1.

Таким образом, все пункты технического задания на выпускную квалификационную работу выполнены в полном объеме.

Список используемых источников

- 1 Ярочкин В.И. Информационная безопасность: Учеб для вузов. Изд.2. Мн.:Академический проект, 2005. - 544с.
- 2 Обзор законодательства Российской Федерации в сфере информационной безопасности— Часть 1: Общий обзор[Электронный ресурс], URL: <https://digital.report/zakonodatelstvo-rossii-informatsionnaya-bezopasnost/>,свободный (дата обращения: 11.05.2020).
- 3 Обзор законодательства Российской Федерации в сфере информационной безопасности — Часть 3: Государственная тайна[Электронный ресурс], URL: <https://digital.report/zakonodatelstvo-rossii-gosudarstvennaya-tayna/>,свободный (дата обращения: 11.05.2020).
- 4 Обзор законодательства Российской Федерации в сфере информационной безопасности — Часть 4: Коммерческая тайна[Электронный ресурс], URL: <https://digital.report/zakonodatelstvo-rossii-kommercheskaya-tayna/>,свободный (дата обращения: 11.05.2020).
- 5СТАНДАРТЫ СОТОВЫХ СЕТЕЙ: ОТ 1G ДО 5G[ЭЛЕКТРОННЫЙ РЕСУРС], URL:[HTTPS://SETPHONE.RU/STATI/STANDARTY-SOTOVYX-SETEJ-OT-1G-DO-5G/](https://setphone.ru/stati/standarty-sotovyyx-setej-ot-1g-do-5g/), СВОБОДНЫЙ (ДАТА ОБРАЩЕНИЯ: 10.05.2020).
- 6 Хорев А.А. Технические каналы утечки информации, обрабатываемой средствами вычислительной техники [Электронный ресурс], URL: <http://www.bnti.ru/showart.asp?aid=954&lvl=04.03>, свободный (дата обращения: 10.05.2020).
- 7Поколения и элементная база ЭВМ[Электронный ресурс], URL: <http://www.docme.ru/doc/929738/%C2%A7-1.-pokoleniya-i-e-lementnaya.../#3>, свободный (дата обращения: 01.05.2020)
- 8 СОВРЕМЕННАЯ ТЕХНИКАИ ТЕХНОЛОГИЯ [Электронный ресурс], URL: <http://portal.tpu.ru/tpu/files/ctt2010-tom1.pdf> , свободный (дата обращения: 11.05.2020).

9Сотовые сети: взлом проще простого [Электронный ресурс], URL: <https://www.kaspersky.ru/blog/hacking-cellular-networks/9862/>, свободный (дата обращения: 11.05.2020).

10Хорев А.А. Защита информации от утечки по техническим каналам. Часть 1. Технические каналы утечки информации [Электронный ресурс], URL: <http://www.analitika.info/kanalutechki.php>, свободный (дата обращения: 01.05.2020).

11Кечиев Л.Н., Степанов П.В. ЭМС и информационная безопасность в системах телекоммуникаций. – М.: Издательский Дом «Технологии», 2005.

12Документ "Руководство пользователя" [Электронный ресурс], URL: http://www.rugost.com/index.php?option=com_content&view=article&id=181&catid=27&Itemid=64, свободный (дата обращения: 11.05.2020).

13Блиялкин, П. А. Выявление электронных устройств перехвата акустической речевой информации, построенных на базе средств беспроводной связи / П. А. Блиялкин, А. В. Смоленков. — Текст : непосредственный // Молодой ученый. — 2016. — № 14 (118). — С. 124-128. — URL: <https://moluch.ru/archive/118/32820/> (дата обращения: 19.05.2020).

14 Уголовный кодекс Российской Федерации" от 13.06.1996 N 63-ФЗ (ред. от 07.04.2020) (с изм. и доп., вступ. в силу с 12.04.2020)[Электронный ресурс], URL: http://www.consultant.ru/document/cons_doc_LAW_10699/, свободный (дата обращения: 11.05.2020).

15Список заболеваний глаз, их симптомы и лечение [Электронный ресурс], URL: <https://zrenie.guru/zabolevaniya-glaz>, свободный (дата обращения: 11.05.2020).

ПриложениеА

(Обязательное)

Протокол проверки ВКР на оригинальность в системе «Антиплагиат»

Протокол проверки на оригинальность в системе «Антиплагиат» (www.antiplagiat.ru) ВКР на тему «Комплекс для выявления закладных устройств, работающих по каналам сотовой связи» студента 5 курса Р.А.Басырова специальности 10.05.03 «Информационная безопасность автоматизированных систем», специализации «Защищенные автоматизированные системы управления» представлен на рисунке А.1.

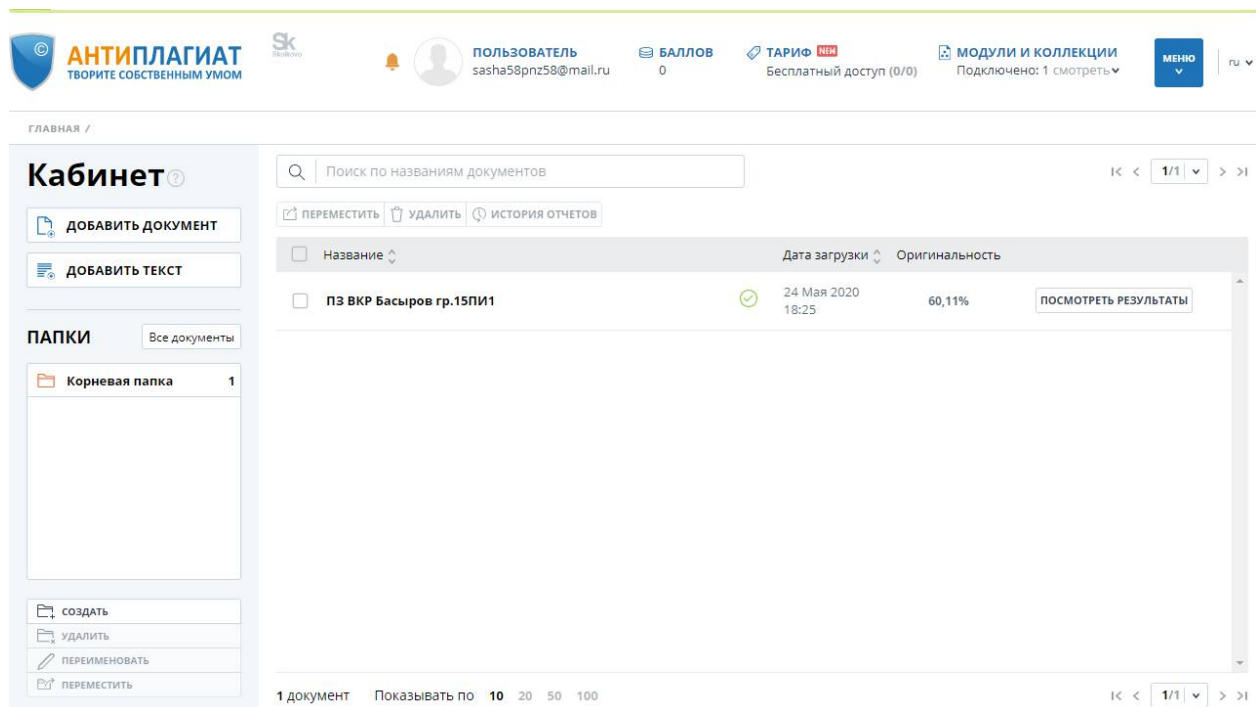


Рисунок А.1 - Протокол проверки ВКР на оригинальность в системе «Антиплагиат»