**МИНИСТЕРСТВО ВЫСШЕГО И СРЕДНЕГО СПЕЦИАЛЬНОГО ОБРАЗОВАНИЯ РЕСПУБЛИКИ УЗБЕКИСТАН**

**МИНИСТЕРСТВО ПО РАЗВИТИЮ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И КОММУНИКАЦИЙ РЕСПУБЛИКИ УЗБЕКИСТАН**

**ТАШКЕНТСКИЙ УНИВЕРСИТЕТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ИМЕНИ МУХАММАДА АЛЬ-ХОРЕЗМИ**

**Ганиев Салим Каримович, Кучкаров Тахир Анварович**

# БЕЗОПАСНОСТЬ СЕТЕЙ

## (БЕЗОПАСНОСТЬ МОБИЛЬНЫХ СЕТЕЙ)

**(Учебное пособие)**

**Ташкент - 2019**

**УДК: 681.3 004.77(057.4)**
**ВВК: 32.973**
**Г 01**

**Ганиев С. К., Кучкаров Т. А. Безопасность сетей (Безопасность мобильных сетей). Ученое пособие - Т.: "Aloqachi", 2019, 169 с.**

Данное учебное пособие подготовлено профессорско-преподавательским составом кафедры "Обеспечение информационной безопасности" Ташкентского университета информационных технологий, являющимся базовым учебным заведением по данному направлению. В нем рассмотрены инфраструктура мобильной сети, беспроводные сети, системы спутниковой связи, угрозы безопасности в мобильных системах, безопасность мобильных операционных систем, уязвимости мобильных приложений, технологии обеспечения безопасности беспроводных и мобильных сетей, обеспечение безопасности в мобильной коммерции, методы защиты информации в облачных вычислениях, аудит и мониторинг безопасности беспроводных сетей.

Учебное пособие предназначено для студентов высших учебных заведений, слушателям групп повышения квалификации, а также лицам, деятельность которых связана с защитой беспроводных и мобильных систем.

**УДК: 681.3 004.77(057.4)**
**ВВК: ББК 32.973**
**Г 01**

**Рецензенты:**

**Парсиев С. С.** - заведующий кафедрой "Аппаратное и программное обеспечение в системе управления телекоммуникаций" ТУИТ, кандидат технический наук, доцент.

**Нигманов А. А.** - начальник отдела развития средств безопасности "Центра информационной и общественной безопасности", кандидат технических наук.

ISBN 978-9943-5521-2-8

## СОДЕРЖАНИЕ

# ВВЕДЕНИЕ

Содержание предмета "Безопасность мобильных сетей" по направлению образования "Информационная безопасность" определяется следующим образом: цель изучения учебной дисциплины - дать студентам современные и перспективные теоретические и практические знания по беспроводным и мобильным технологиям. Изучение учебной дисциплины включает пользование средой передачи информации, топологии, стандартов, технологий, вопросы безопасности. В этой же дисциплине рассматриваются такие проблемы, как нарушение целостности информации, несанкционированное использование беспроводных и мобильных информационных сетей, нарушение их занятости.

Знание основ радиосвязи, радиоэлектронных систем, распространение радио - это первый шаг в освоении предмета.

В связи с этим *первая глава* учебника посвящена рассмотрению типам радиосигналов и их основных характеристик, влиянию многолучевости при распространении сигнала разной частоты, спектральному распределению частот, изучению большинства пользовательских типов систем.

*Во второй главе* освещены принципы построения мобильных систем, структура компонентов мобильной сети, частотно-временное распределение в мобильных системах, особенности и основы построения мобильных систем.

*Третья глава* посвящена вопросам создания локальных, городских и глобальных беспроводных систем и сетей, обеспечивающих широкополосный доступ.

*В четвертой главе* рассматриваются методы использования спутниковых систем мобильной связи, принципы их построения, структурные и ключевые характеристики, а также использование спутниковой мобильной связи в интернет-технологиях.

*В пятой главе* представлены классификация угроз информационной безопасности, основные угрозы информационной безопасности в мобильных системах, модель информационной безопасности злоумышленника.

*В шестой главе* рассмотрены механизмы обеспечения безопасности в различных операционных системах. Представлен сравнительный анализ механизмов обеспечения безопасности широко используемых в мире операционных систем Android и iOS.

*Глава седьмая* посвящена угрозам и уязвимостям в мобильных приложениях. Приведена классификация угроз и уязвимостей для мобильных приложений. Приведены примеры уязвимостей мобильных приложений, а также методы защиты мобильных приложений, рассмотрены анализ и оценка угроз.

Содержание *восьмой главы* - это технологии, которые обеспечивают безопасность, как в беспроводных, так и в мобильных сетях. Для беспроводных и мобильных сетей технологии защиты информации рассматривались с использованием базового стандарта IEEE 802.11 (Wi-Fi 802.11), стандартов EAP и IEEE 802.1 x, протоколов IPSec. Рассмотрен также стандарт IEEE 802.11i, обеспечивающий всестороннюю безопасность.

*В девятой главе* даны рекомендации по повышению информационной безопасности при использовании моделей мобильных финансовых услуг, существующих угроз и уязвимостей при осуществлении мобильных платежей, а также методы повышения безопасности при мобильных платежах.

*Десятая глава* посвящена мобильным облачным технологиям. Рассмотрены архитектура взаимодействия облачных вычислительных систем с мобильными приложениями, проблемы использования облачных вычислений в мобильных технологиях, возможности мобильных агентов в модели облачных вычислений. Приведены анализ угроз при выпонении облачных вычислений а также методы защиты от них.

*Одиннадцатая глава* посвящена аудиту и мониторингу безопасности мобильных систем.

# ГЛАВА 1. КРАТКИЕ СВЕДЕНИЯ О ПРИНЦИПАХ РАДИОСВЯЗИ

## 1.1. Типы радиосигналов и их характеристики

Передача сообщений на расстояние без проводов осуществляется с помощью ***электромагнитных волн (радиоволн)***, распространяющихся в пространстве электромагнитных полей. Электромагнитное поле - это совокупность переменных электрического и магнитного полей. Основной характеристикой электрического поля является его напряженность *E*, которая представляет собой силу, действующую со стороны поля на единичный положительный электрический заряд. Напряженность электрического поля зависит от диэлектрической проницаемости *e* среды, в которой существует поле. Величина *E* показывает, во сколько раз напряженность электрического поля в данной среде отличается от напряженности поля в вакууме.

Основной характеристикой магнитного поля является его напряженность *H*, представляющая собой отношение магнитной индукции *B* к магнитной проницаемости *m* среды, в которой существует поле. Индукцией магнитного поля называется сила, действующая со стороны поля на единичный положительный электрический заряд, движущийся с единичной скоростью перпендикулярно к магнитным силовым линиям. Величина m показывает, во сколько раз индукция магнитного поля в данной среде отличается от индукции поля в вакууме.

Величины *E* и *H* являются векторными, т.е. величинами, которые характеризуются не только числовыми значениями, но и направлением. Векторы *E* и *H* перпендикулярны друг другу и направлению распространения волны. Ориентировка в пространстве вектора *E* определяет поляризацию радиоволны. Различают линейную, круговую и эллиптическую поляризации.

Радиоволна называется линейно поляризованной, если вектор электрического поля *E* в каждой точке вдоль линии распространения лежит в одной плоскости, называемой плоскость поляризацией. В зависимости от расположения плоскости поляризации различают вертикальную и горизонтальную поляризацию. При круговой поляризации конец вектора электрического поля с течением времени описывает окружность, а при эллиптической – эллипс.

На рис. 1.1 изображены графики изменения в пространстве напряженностей электрического и магнитного полей электромагнитной волны, распространяющейся в направлении OX, и имеющей вертикальную линейную поляризацию.

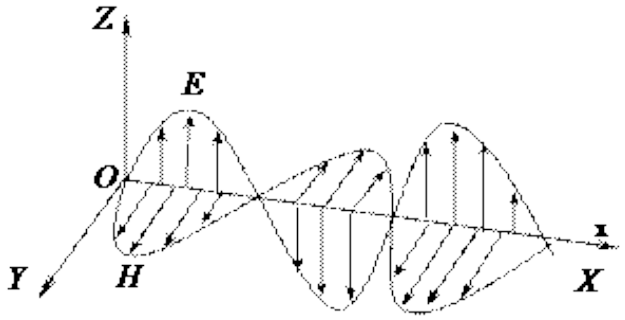



Рис.1.1. Структура электромагнитной волны

Радиосигналами называют электромагнитные волны или электрические высокочастотные колебания, которые заключают в себе передаваемое сообщение. Для образования сигнала параметры высокочастотных колебаний изменяются (модулируются) с помощью управляющих сигналов, которые представляют собой напряжение, изменяющееся по заданному закону. В качестве модулируемых обычно используются высокочастотные гармонические колебания:

$$u(t) = U_0 \sin(\omega_0 t), \qquad (1.1)$$

где $w_0=2\pi f_0$ – высокая несущая частота;

$U_0$ – амплитуда высокочастотных колебаний.

К наиболее простым и часто используемым управляющим сигналам относятся гармонические колебания

$$U_{\text{гарм}}(t) = U_m sin(\Omega t - \Psi)\ , \qquad (1.2.)$$

где Ω – низкая частота, много меньшая $w_0$; ψ – начальная фаза; $U_m$ – амплитуда, а также прямоугольные импульсные сигналы, которые характеризуются тем, что значение напряжения $U_{упр(t)}=U$ в течение интервалов времени $\tau_и$, называемых длительностью импульсов, и равно нулю в течение интервала между импульсами (рис.1.2). Величина $T_и$ называется периодом повторения импульсов; $F_и=1/T_и$ – частота их повторения. Отношение периода повторения

импульсов $T_и$ к длительности $\tau_и$ называется скважностью Q импульсного процесса: $Q=T_и/\tau_и$.

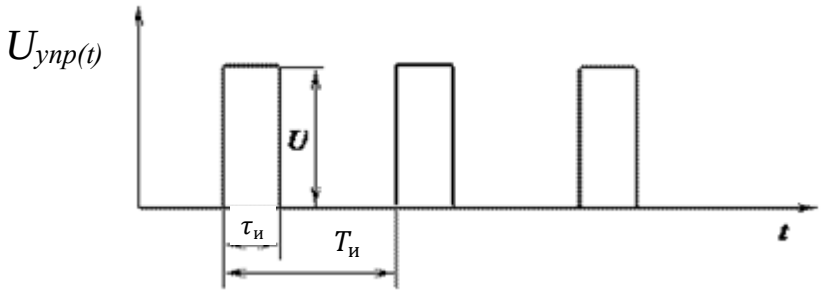



Рис.1.2. Последовательность прямоугольных импульсов

В зависимости от того, какой параметр высокочастотного колебания изменяется (модулируется) с помощью управляющего сигнала, различают амплитудную, частотную и фазовую модуляции.

При передаче последовательности импульсов, например, двоичного цифрового кода (рис.1.3,а), также может использоваться АМ, ЧМ и ФМ.

При амплитудной модуляции образуется последовательность высокочастотных радиоимпульсов, амплитуда которых постоянна в течение длительности модулирующих импульсов $\tau_и$, и равна нулю все остальное время (рис.1.3,б).

При частотной модуляции образуется высокочастотный сигнал с постоянной амплитудой, и частотой, принимающей два возможных значения (рис.1.3,в).

При фазовой модуляции образуется высокочастотный сигнал с постоянной амплитудой и частотой, фаза которого изменяется на 180° по закону модулирующего сигнала (рис.1.3,г).

Сигнал на пути от передатчика к приемнику редко распространяется по прямой линии. На пути распространения обычно попадаются различные препятствия, которые ведут к отражениям сигнала и изменению его траектории. В результате может сложиться ситуация когда к приемнику будут поступать не одна а сразу несколько сдвинутых по времени копий исходного сигнала с разными амплитудами. Причем энергия исходного сигнала будет распределена между копиями неравномерно. Это так называемое явление ***многолучевого распространения сигнала***. Рассмотрим простую модель распространения радиосигналов в системе мобильной связи

называемую двухлучевой моделью распространения радиоволн (рис.1.4).

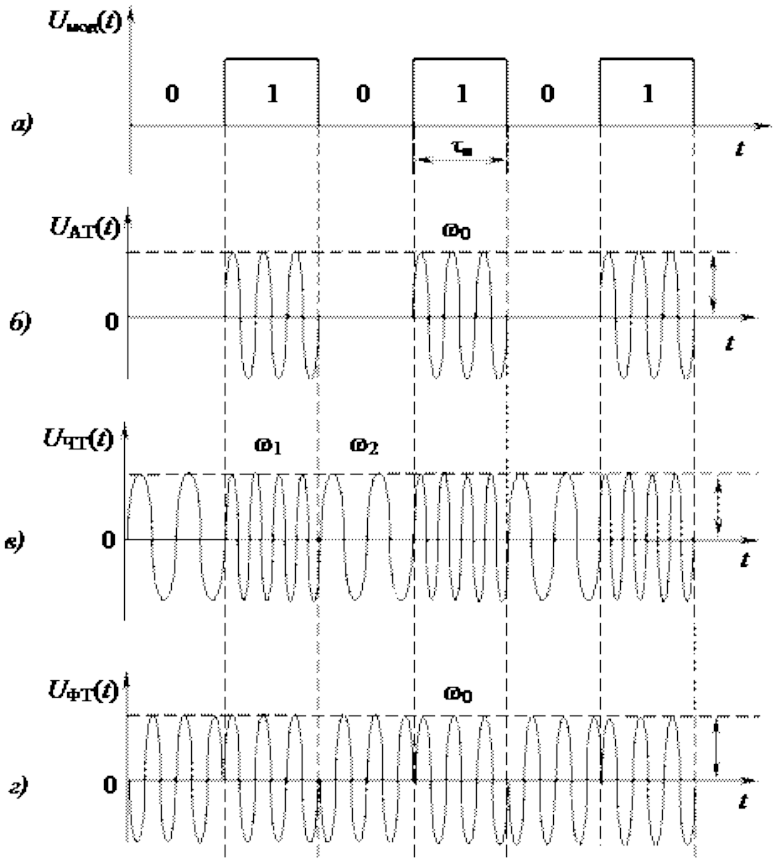



Рис.1.3. Сравнительный вид манипулированных колебании при АМ, ЧМ и ФМ

Пусть передающая и приемная антенны расположены соответственно на высотах $h_1$ и $h_2$ над уровнем земли. Расстояние между обеими антеннами вдоль земли равно $r$ и намного превышает высоты обеих антенн. Предположим, что сигнал попадает на вход приемника двумя путями: прямым (по линии прямой видимости $r_1$) и с одним отражением от земли (ломаная линия $r_2$). Примем что, отражение от поверхности земли происходит без потерь, т.е. энергия падающей волны равно энергии отраженной волны. Можно доказать что, при таком подходе мощность на входе приемника будет определяться выражением:

$$P_{ПРМ}(r) = G_{ПРД.А} G_{ПРМ.А} P_{ПРД} \frac{h_1^2 h_2^2}{r^4}. \qquad (1.3)$$

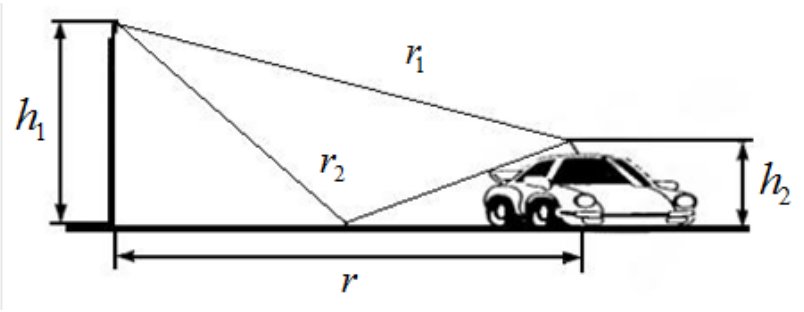



Рис. 1.4.

где:

$G_{ПРД}$ - коэффициент усиления передающей антенны;

$P_{ПРД.А}$ - мощность излучения антенны;

$P_{ПРМ} = \Pi \cdot S_д$ - часть излучаемой мощности передающей антенны, принимаемая приемной антенной и зависящая от диаметра приемной антенны (Sd).

Частотный диапазон радиоволн используемых в технике показан на рис. 1.5.

Длина радиоволны (λ) – это расстояние между двумя ближайшими друг к другу точками, колеблющимися в одинаковых фазах.

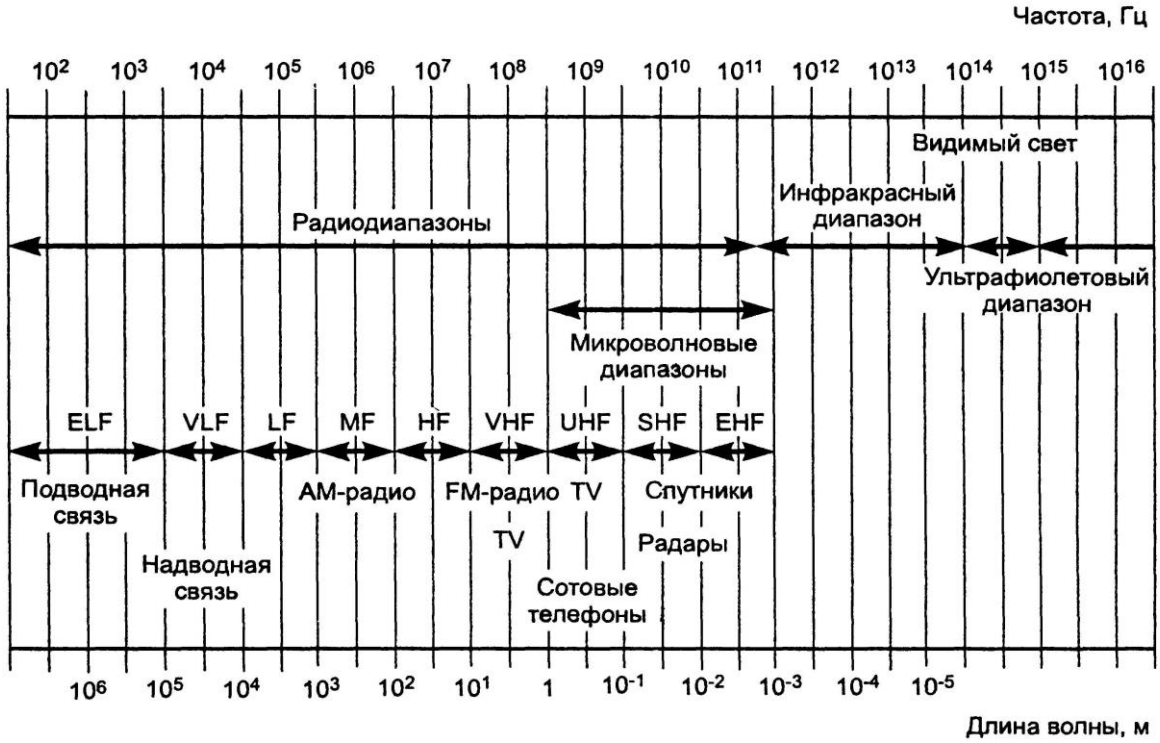



Рис. 1.5. Частотный диапазон волн

Длину радиоволны можно рассчитать следующим образом: 300 (скорость света в мегаметрах в секунду) делим на частоту в

мегагерцах, получаем длину волны в метрах, например, для 600 МГц, длина волны равна 0,5 метра.

## 1.2. Методы организации радиосвязи

Выбор способа передачи и приема информации и техническая реализация являются основными проблемами построения системы связи.

Эти вопросы неразрывно связаны с такими процессами, как модуляция и демодуляция.

Любая система связи устроена таким образом, что при использовании имеющихся ресурсов, таких как время, частота, энергия, динамический диапазон обеспечивается передача большей части пространственной информации с заданным качеством связи и допустимым минимальным потреблением энергии.

В настоящее время аналоговая передача информации не используется. Потому что современная микроэлектроника позволяет реализовать достаточно сложные алгоритмы обработки цифровых сигналов. Кроме того, цифровых систем по сравнению с аналоговыми системами.

Можно выделить следующие характеристики цифровых систем:

- сообщения, значения которых передаются в виде последовательности бит получателя;

качество передачи сообщений выше во всех остальных общих условиях

- последовательность битов передается одним из сигналов, который называется канальными сигналами.

Система связи, которая обеспечивает передачу сообщений от одного источника к одному приемнику через одну линию связи называют одноканальной. Схема структура одноканальной системы связи представлена на рисунке 1.6.

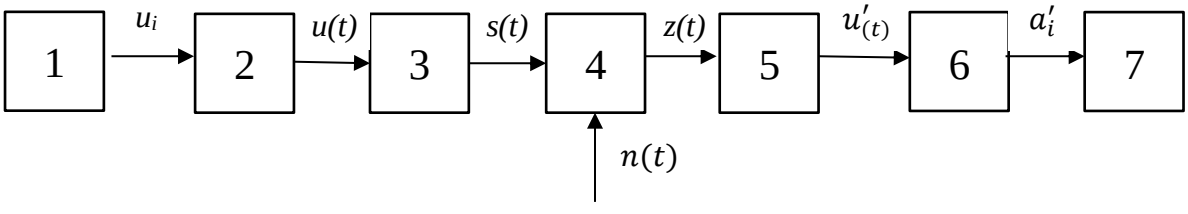



Рис. 1.6. Структурная схема одноканальной системы связи

Здесь:

1 - источник сообщения - лицо или техническое устройство, которое формирует сообщение передатчика $u_i$ ;

2 - преобразователь сообщения в сигнал - устройство преобразования сообщения в первичный сигнал низкой частоты *u(t)*;

3 - передатчик - преобразователь первичного низкочастотного сигнала во вторичный высокочастотный *s(t)* для передачи его по линии связи;

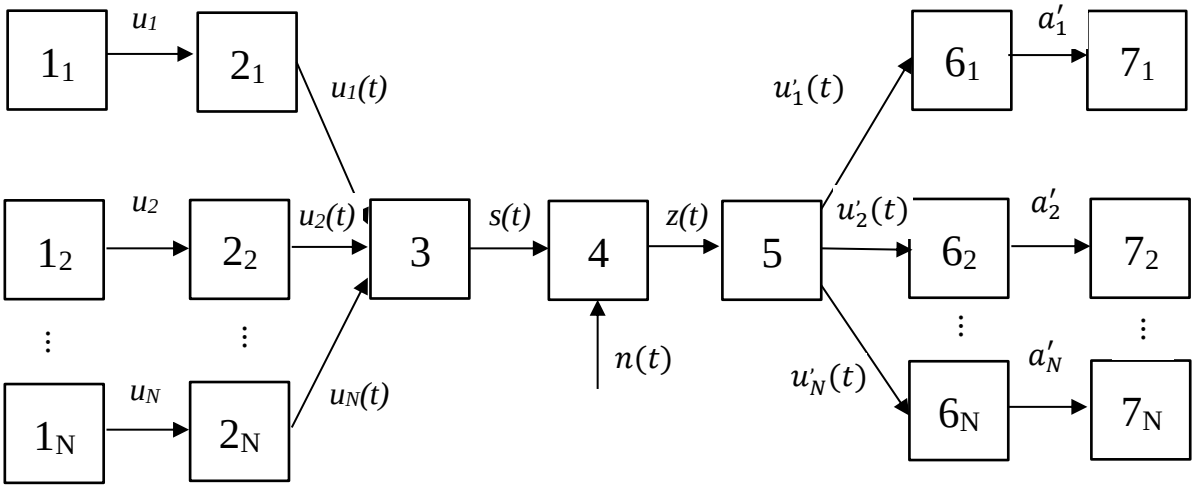
4 - линия связи - среда, используемая для передачи сигнала от передатчика к приемнику. При прохождении линии связи электрические сигналы подвержены $n(t)$ помехам и искажениям. $z(t)$ - сигнал на выходе линии связи может отличаться от переданного сигнала $a_i$ и полученного сообщения;

5 - приемник сигнала - устройство, восстанавливающее первичный сигнал $u'_{(t)}$ из полученного вторичного высокочастотного сигнала;

6 - преобразователь полученного сигнала в сообщение $a'_i$.

7 - получатель сообщения - человек или устройство, которое воспринимает сообщение.

Система связи, которая обеспечивает одновременную передачу сообщений от нескольких источников к нескольким получателям через одну общую линию связи, называется многоканальной. Схема структуры многоканальной системы связи представлена на рисунке 1.7.




1.7. Структурная схема многоканальной системы связи

Здесь:

$1_i$ - источник сообщений - лицо или техническое устройство, формирующее передаваемое сообщение $u_i$ ;

$2_i$ – преобразователь сообщения в первичный низкочастотный сигнал $u_i(t)$ - сообщение в основной, низкочастотный;

3 - преобразователь сигнала (передатчик). Первичные сигналы $u_i(t)$ в этом устройстве по каналам связи, затем объединяются в групповой сигнал, который направляется на линию связи:

$$S(t) = \sum_{1=i}^{N} s_i(t), \qquad (1.4)$$

здесь:

$s(t)$ - канальные сигналы - сигналы, которые имеют определенные отличительные признаки (характер активности), что позволяет разделить их тем или методом (разделение по уровню, комбинированные системы с использованием частотного и (или) временного разделения) на первичные сигналы $u_i(t)$;

$N$ - количество каналов в системе.

4 - линия связи - среда используемая при передаче сигналов от передатчика к приемнику. При прохождении через линию связи электрические сигналы подвергаются $n(t)$ помехам и нарушениям. Это приводит к разнице в сигнале на выходе $z(t)$ линии связи и полученном сообщении $a_i'$ соответственно от сигнала на входе линии связи и от сообщения передачи.

5 - преобразователь сигнала (приемник). Выделяет из переданного группового сигнала $s_i'(t)$ первичные сигналы $u_i'(t)$;

$6_i$ - это устройство, преобразует полученные сигналы в сообщения $a'_i$;

$7_i$ - это лицо или техническое устройство, которое получает сообщение.

В настоящее время в системах с подвижными объектами используется 3 основных способа множественного доступа:

- TDMA (Time Division Multiple Access) – множественный доступ с временным разделением;
- FDMA (Frequency Division Multiple Access) – множественный доступ с частотным разделением;
- CDMA (Code division multiple access) – множественный доступ с кодовым разделением.

Основной принцип TDMA заключается в том, что имеющийся ресурс разделяется между участниками информационного обмена на циклически повторяющиеся промежутки времени. Промежутки времени получили название "таймслот" (timeslot, TS) (рис. 1.8). При этом абонент может использовать всю ширину пропускания канала, но только в определенные временные отрезки (рис. 1.9).

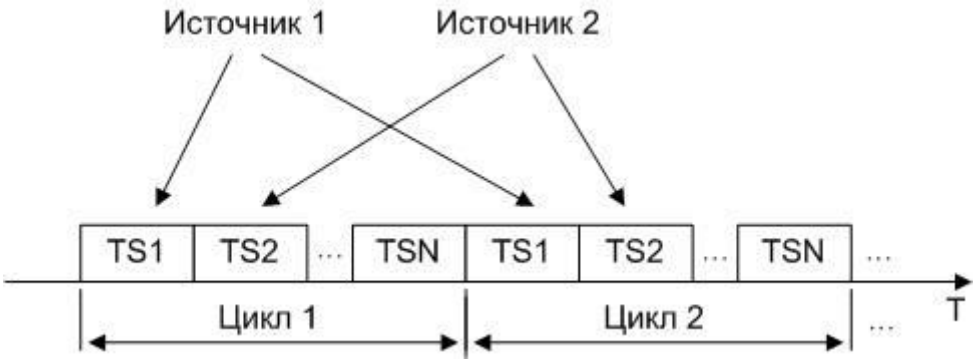



Рис. 1.8. Структура цикла TDMA

В такой ситуации главное, чтобы сигналы соседних таймслотов не накладывались друг на друга. Это может быть вызвано как слишком высокой мощностью передачи, так и помехами в канале, несовершенством используемого оборудования. Чтобы избежать подобных межслотовых помех часто вводят специальный защитный временной интервал. Таким образом, если часть энергии одного передатчика просочится за пределы отведенного ему таймслота, то она будет оказывать воздействие лишь на не несущий информацию защитный интервал. Введение такого интервала снижает общую пропускную способность канала связи, но необходимо для поддержания заданных характеристик качества обслуживания.


Рис. 1.9. Защитные интервалы в цикле TDMA

TDMA применяется в стандарте сотовой связи GSM (Global System for Mobile Communications).

Принцип FDMA заключается в том, что весь частотный спектр разделяется между пользователями на равные или не равные частотные полосы. Источники информации могут использовать выделенный им частотный ресурс неограниченно по времени, но при этом не должны создавать помехи соседним каналам. Чтобы избежать переходных помех вводят специальный защитный частотный интервал между соседними каналами. Это так называемая полоса расфильтровки. Она не используется для передачи информации и поэтому снижает общую пропускную способность имеющегося канала связи.

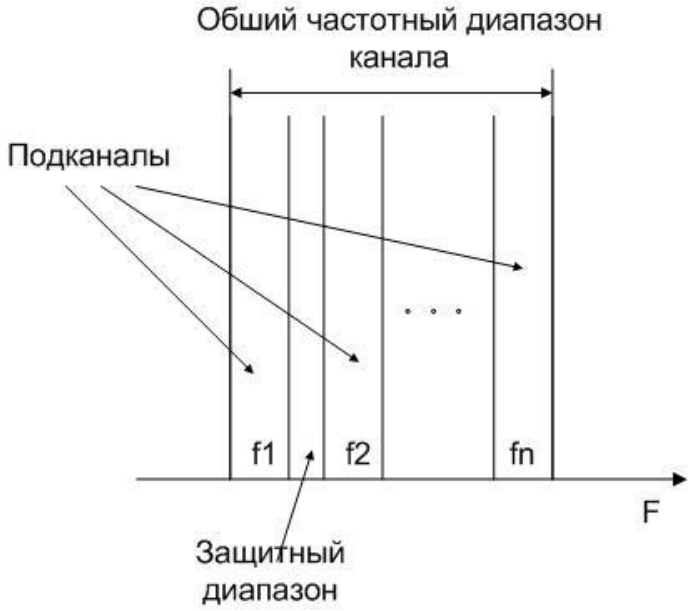



Рис. 1.10. Принцип организации FDMA

Как и в принципе временного разделения, где используется не все отведенное время (защитный временной интервал), принцип частотного разделения, когда ресурс доступен неограниченно по времени, не в полной мере использует весь частотный диапазон.

Это обусловлено двумя причинами:

1. Нельзя передавать сигналы без высокочастотной модуляции, так как сигнал быстро затухает в передающей среде.

2. Частоты и время – это также ресурсы, которые используется для увеличения объема передачи данных.

Поэтому при организации связи используется сразу оба принципа. Например, в стандарте GSM одновременно используются TDMA и FDMA. Весь частотный диапазон разделяется на частотные

каналов по 200 кГц каждый, которые в свою очередь состоят из 8 таймслотов.

В CDMA (Code Division Multiple Access), для каждого узла выделяется весь спектр частот и всё время. Все передатчики передают сигналы на одной и той же частоте, области пространства и одинаковые моменты времени, но с разными кодами. Каждый передатчик заменяет каждый бит исходного потока данных на CDM-символ - кодовую последовательность длиной в 8, 16, 32, 64 и т.п. бит (их называют чипами). Кодовая последовательность уникальна для каждого передатчика. Как правило, если для замены «1» в исходном потоке данных используют некий CDM-код, то для замены «0» применяют тот же код, но инвертированный. Приемник знает CDM-код передатчика, сигналы которого должен воспринимать.

Каналы трафика при таком способе разделения среды создаются посредством применения широкополосного кодо-модулированного радиосигнала – шумоподобного сигнала, передаваемого в общий для других аналогичных передатчиков канал, в едином широком частотном диапазоне (рис. 1.11).

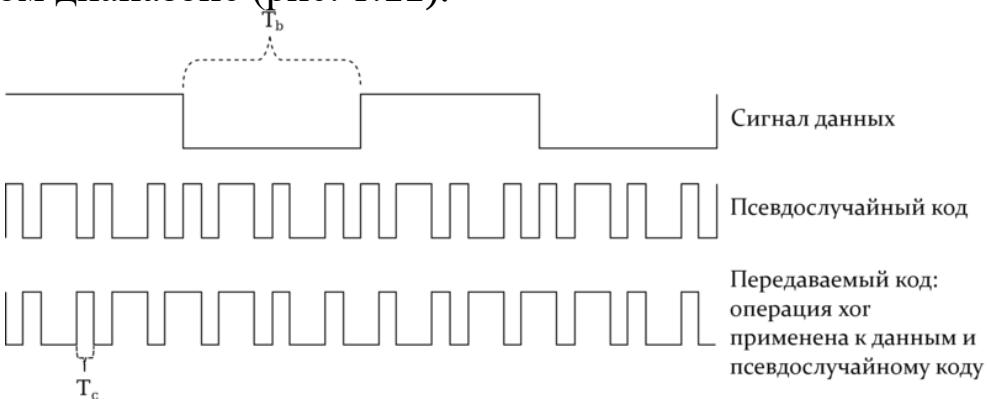



Рис. 1.11. Генерация сигнала CDMA

В результате работы нескольких передатчиков эфир в данном частотном диапазоне становится ещё более шумоподобным.

Каждый передатчик модулирует сигнал с применением присвоенного в данный момент каждому пользователю отдельного числового кода, приёмник, настроенный на аналогичный код, может вычленять из общей какофонии радиосигналов ту часть сигнала, которая предназначена данному приёмнику. В явном виде отсутствует временное или частотное разделение каналов, как в TDMA или FDMA, каждый абонент постоянно использует всю ширину канала, передавая сигнал в общий частотный диапазон, и принимая сигнал из общего частотного диапазона. При этом

широкополосные каналы приёма и передачи находятся на разных частотных диапазонах и не мешают друг другу. Полоса частот одного канала очень широка, вещание абонентов накладывается друг на друга, но, поскольку их коды модуляции сигнала отличаются, они могут быть дифференцированы аппаратно-программными средствами приёмника.

Все вышесказанное позволяет говорить о высокой эффективности CDMA, т.к. кодовое разделение, применяемое в CDMA, позволяет обслуживать больше абонентов на той же полосе частот, чем другие виды разделения (TDMA, FDMA). При кодовом разделении нет строгого ограничения на число каналов. С увеличением числа абонентов постепенно возрастает вероятность ошибок декодирования, что ведёт к снижению качества канала, но не к отказу обслуживания. CDMA имеет более высокую защищённость каналов. Выделить нужный канал без знания его кода весьма трудно. Телефоны CDMA имеют меньшую пиковую мощность излучения, и потому менее вредны.

# ГЛАВА 2. ИНФРАСТРУКТУРА МОБИЛЬНЫХ СЕТЕЙ

## 2.1. Компоненты мобильных сетей

Основные компонентами мобильной сети являются - цифровая мобильная станция, базовая станция и центр коммутации.

Упрощенная блок-схема *цифровой мобильной станции*, иначе говоря, современного мобильного телефона изображена на рис. 2.1.

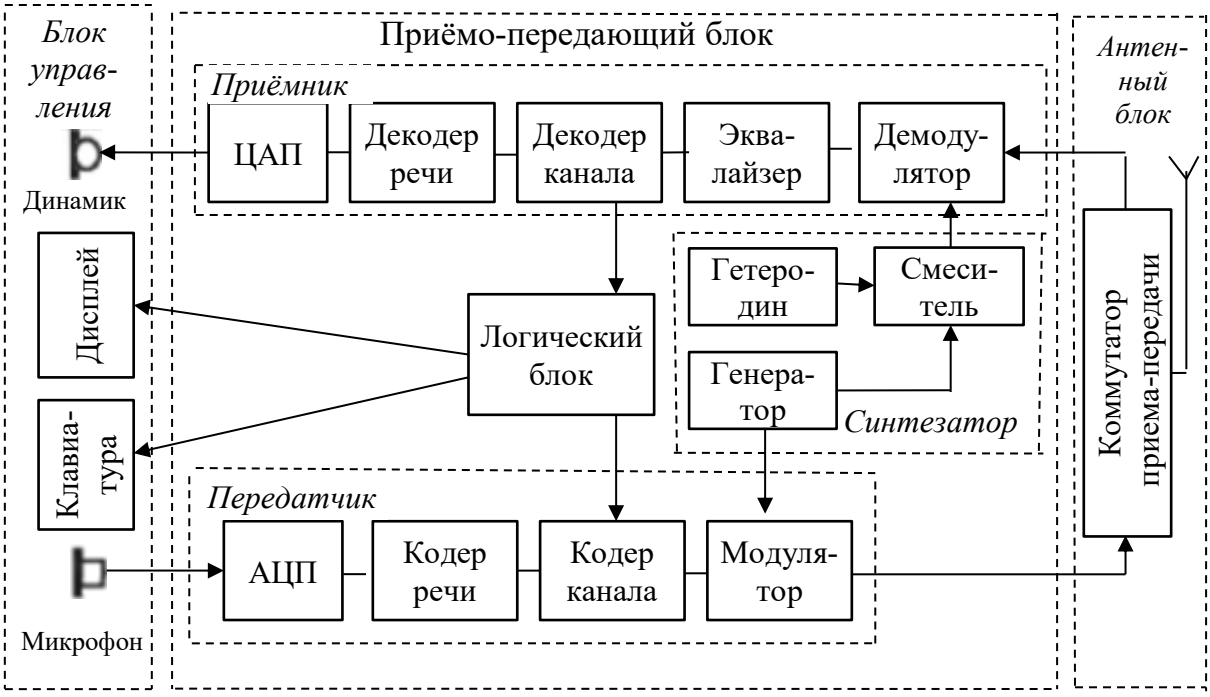



Рис. 2.1. Блок-схема цифровой мобильной станции

*Блок управления* включает в себя микрофон и динамик, клавиатуру и дисплей. Клавиатура предназначена для набора номера телефона вызываемого абонента, а также команд, определяющих режим работы станции. Дисплей предназначен для отображения информации.

*Приемо-передающий блок* состоит из передатчика, приемника, синтезатора частот и логического блока.

В состав передатчика входят:

- аналого-цифровой преобразователь (АЦП) - преобразует в цифровую форму сигнал с выхода микрофона (вся последующая обработка и передача сигнала речи производится в цифровой форме);
- кодер речи - с целью сокращения его избыточности;
- кодер канала - осуществляет кодирование передаваемого сигнала с целью защиты от ошибок при передаче по радиоканалу, а

также вводит в состав передаваемого сигнала информацию управления, поступающую от логического блока; осуществляет кодирование сигнала речи, т. е. преобразование цифрового сигнала.

- модулятор - осуществляет перенос информации кодированного видеосигнала на несущую частоту.

Приемник по составу соответствует передатчику, но с обратными функциями входящих в него блоков:

- демодулятор - выделяет из модулированного радиосигнала кодированный видеосигнал, несущий информацию;
- эквалайзер предназначен для компенсации искажений сигнала из-за многолучевого распространения;
- декодер канала - обнаруживает и исправляет ошибки в принятом сигнале, а также выделяет из входного потока и направляет в логический блок управляющую информацию;
- декодер речи - восстанавливает сигнал речи в цифровом виде;
- цифро-аналоговый преобразователь (ЦАП) преобразует принятый цифровой сигнал речи в аналоговую форму и подает его на вход динамика;
- логический блок - это микрокомпьютер, осуществляющий управление работой мобильной станции (МС).

*Антенный блок* включает в себя антенну (обычно находится внутри мобильного устройства) и электронный коммутатор приема – передачи, подключающий антенну либо на выход передатчика, либо на вход приемника, так как МС цифровой системы никогда не работает на прием и передачу одновременно.

Для обеспечения конфиденциальности передачи информации в некоторых системах используется режим шифрования, в этих случаях передатчик и приемник МС включают соответственно блоки шифратора и дешифратора сообщений.

В МС предусмотрен также специальный съемный модуль идентификации абонента (Subsriber Identity Module - SIM). Мобильная станция включает и детектор речевой активности VAD (Voice Activity Detector). VAD включает передатчик на излучение только на те интервалы времени, когда абонент говорит. Этим экономится энергия источника питания, снижается уровень помех, создаваемых для других станций при работающем передатчике.

Одной из особенностей организации связи с мобильными абонентами для повышения качества приема на базовой станции (БС) применяют разнесенный прием. Это обусловливает необходимость

установки на БС не менее двух приемных антенн. Кроме того, БС может иметь раздельные антенны на передачу и на прием. Еще одна особенность БС - наличие нескольких приемников и такого же числа передатчиков для обеспечения одновременной работы на нескольких каналах с различными частотами. Блок-схема базовой станции приведена на рис. 2.2.

Число приемо-передатчиков N определяется конструкцией и комплектацией БС. Для обеспечения одновременной работы N приемников на одну приемную и N передатчиков на одну передающую антенну между приемной антенной и приемниками устанавливается делитель мощности на N выходов, а между передатчиками и передающей антенной - сумматор мощности на N входов.

Контроллер БС (компьютер) обеспечивает управление работой станции, а также контроль работоспособности всех входящих в нее блоков и узлов.

Блок сопряжения с линией связи осуществляет упаковку информации, передаваемой по линии связи на центр коммутации подвижной связи (ЦКПС), и распаковку принимаемой от него информации. Для связи БС с ЦКПС (обычно используется радиорелейная или волоконно-оптическая линия.

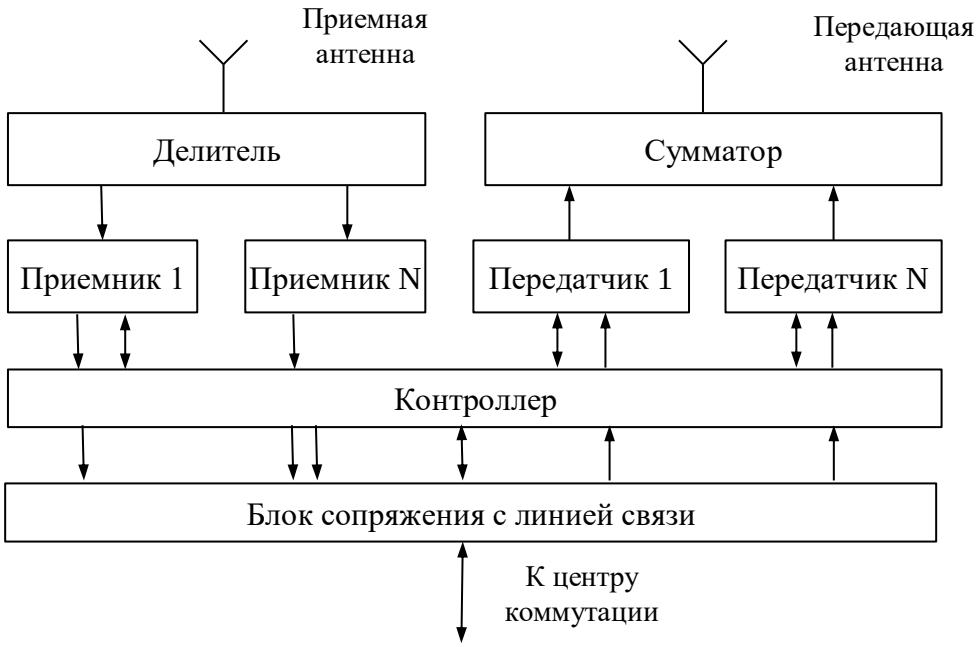



Рис. 2.2. Блок-схема базовой станции

Для обеспечения надежности многие блоки и узлы БС резервируются (дублируются), в состав станции включаются автономные источники бесперебойного питания (аккумуляторы).

Центр коммутации подвижной связи представляет собой специализированный центр электронной коммутации, к которому добавлены функциональные блоки (регистры), решающие задачи, характерные для системы сотовой подвижной связи (рис. 2.3).

*Домашний регистр местоположения ДРМ (HLR - Home Location Register)* - база данных подвижных станций, постоянно зарегистрированных в системе конкретного оператора. Также содержит информацию о наборе услуг предоставляемых каждому абоненту. В данном регистре фиксируется местоположение абонента для организации его вызова, и регистрируются фактически оказанные услуги.

*Центр аутентификации ЦА (AUC - Authentication Center)* - база данных, позволяющая определить - разрешен ли допуск к услугам системы абоненту, имеющему данный модуль подлинности - SIM-карту (Subscriber Identity Module).

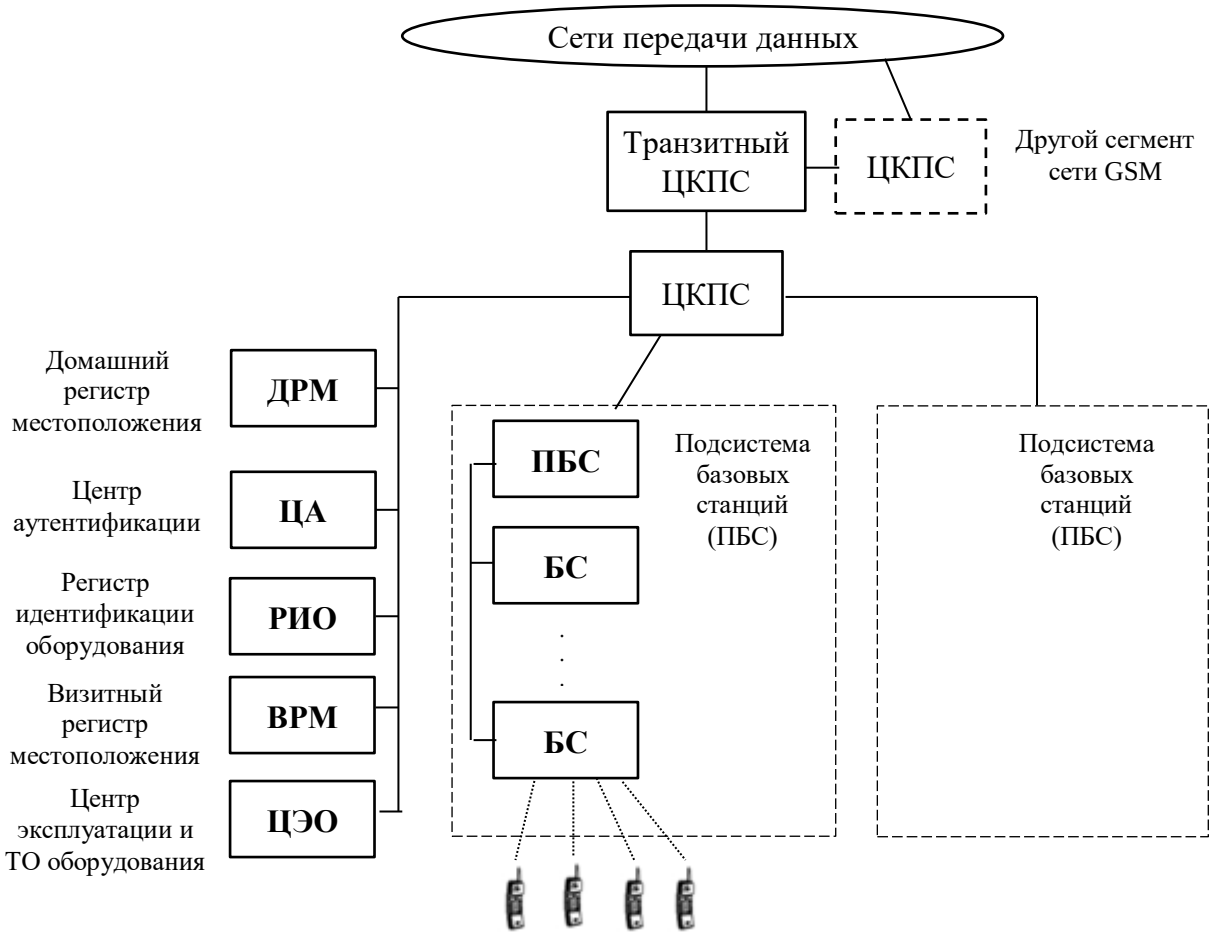



Рис. 2.3. Блок-схема центра коммутации подвижной связи

*Регистр идентификации оборудования РИО (EIR - Equipment Identification Register)* - база данных серийных номеров подвижных станций, используемых в системе. Номера украденных или потерянных телефонов помещаются в "черный список", что позволяет предотвратить дальнейшее использование в системе этих телефонов.

*Визитный регистр местоположения ВРМ (VLR - Visitor's Location Register)* - регистр содержит необходимую информацию о подвижных станциях, временно расположенных в области обслуживания данного оператора (роуминг).

*Центр эксплуатации и технического обслуживания ЦЭО (ОМС - Operating and Maintenance Center)* обеспечивает работу отдельных элементов сети.

Все ЦКПС в сети соединены друг с другом. Один или более ЦКПС, называемые "транзитными центрами коммутации подвижной связи" (транзитные ЦКПС) играют роль шлюзов во внешние сети, например, телефонные сети общего назначения.

Каждый ЦКПС контролирует, по крайней мере, одну подсистему базовых станций ПБС. Базовая станция (БС) состоит из подсистемы выполняющей основные функции передачи и приема сигналов, а также блока, реализующего простые функции контроля и управления. В БС выполняются процедуры кодирования/декодирования речи и производится адаптация скорости передачи данных. Базовые станции обычно располагаются в центрах сот, покрывающих всю область обслуживания системы. В таких сотах функционирует определенное количество подвижных станций (ПС) или (мобильных станций, MS (Mobile Station), имеющих возможность динамически изменять свое местоположение. Они осуществляют информационный обмен с ближайшей (или с сильнейшей) базовой станцией.

Основная задача подсистемы базовых станций заключается в координации установления соединения между двумя мобильными абонентами системы или между одним пользователем системы и абонентом внешней сети.

## 2.2. Структура частотного и временного распределения в мобильных системах

Рассмотрим структуру распределения частот на примере стандарта GSM 900, т.к. именно он является базовой спецификацией

GSM. Стандарт предусматривает работу передатчиков в двух диапазонах частот каждый шириной в 25 МГц (рис. 2.4):

1. Полоса частот 890-915 МГц - для передачи сообщений с МС на БС (uplink);

2. Полоса частот 935- 960 МГц - для передачи сообщений с БС на МС (downlink).

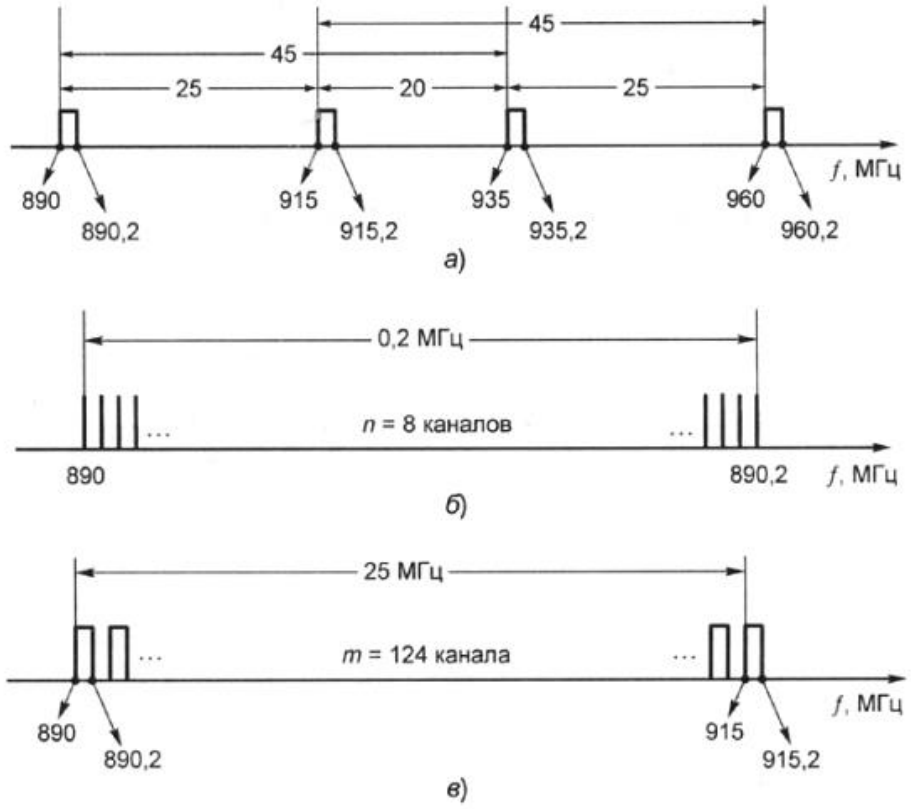



Рис. 2.4. а) разнос между частотами в направлении МС-БС и в направлении БС-МС; б) число физических речевых радиоканалов в дуплексном радиоканале; в) число физических дуплексных речевых радиоканалов.

Как видим, дуплексная передача данных осуществляется в режиме *FDD (Frequency Division Duplex - дуплексная передача с частотным разделением).* При переключении каналов во время сеанса связи разность между этими частотами (между частотами двух диапазонов, а не соседними частотами) постоянна и равна 45 МГц. Разнос частот между соседними каналами связи составляет 200 кГц. Таким образом, в отведенной для приема/передачи полосе частот шириной 25 МГц размещаются 124 канала связи.

В стандарте GSM используется многостанционный доступ FDMA/TDMA, т.е. с частотно-временным разделением каналов, что

позволяет на одной несущей частоте разместить 8 речевых каналов одновременно.

Такую структуру распределения частот в системе GSM можно экстраполировать к любой из вышеперечисленных спецификаций.

Основная временная единица в стандарте GSM называется слот. Восемь временных слотов образуют кадр.

Рассмотрим, как распределяются сигналы во временном слоте. Наименьший временной элемент системы GSM – это одиночный двоичный импульс (бит), длящийся 3,69 мкс. Скорость передачи данных в системе GSM составляет 270,833 Кбит/с. В каждом временном слоте передается пакет из 148 битов. Длительность стандартного временного слота составляет 577 мкс. Разница между фактической длиной слота и эффективной длиной пакета данных называется защитным интервалом. Его существование обусловлено необходимостью резервирования времени для включения/выключения усилителя мощности передатчика в начале и в конце передачи каждого пакета данных. Кроме того, защитный интервал необходим для обеспечения точного размещения пакета данных внутри временного слота.

Структура временного слота состоит из:

*T - Tail bit (хвостовые биты).* Повторяется два раза. Необходимы как защитные бланки по краям пакета;

*S - Stealing flag (скрытые флажки).* Повторяется два раза. Определяет тип передаваемой информации, т.к. она может как пользовательской так и служебной;

*TS - Training Sequence* (обучающая последовательность). Предназначен для оценки качества связи, определения задержек информации между БС и МС;

G- Guard period (защитный интервал).

Восемь слотов составляют кадр. Каждый слот соответствует своему каналу речи, т.е. в каждом кадре передается информация восьми речевых каналов (рис. 2.5).

В каналах трафика (пользовательский кадр) и в ассоциированных с ними каналах управления (служебный кадр) 26 кадров образуют мультикадр. В свою очередь, 51 мультикадр составляет суперкадр длительностью 6,12 с. В обоих случаях 2048 суперкадров образуют высший уровень временной иерархии системы GSM - гиперкадр (рис. 2.6). Он длится 3 ч 28 мин 53 сек 760 мс. По

истечении этого времени системные часы возвращаются к своему исходному состоянию.

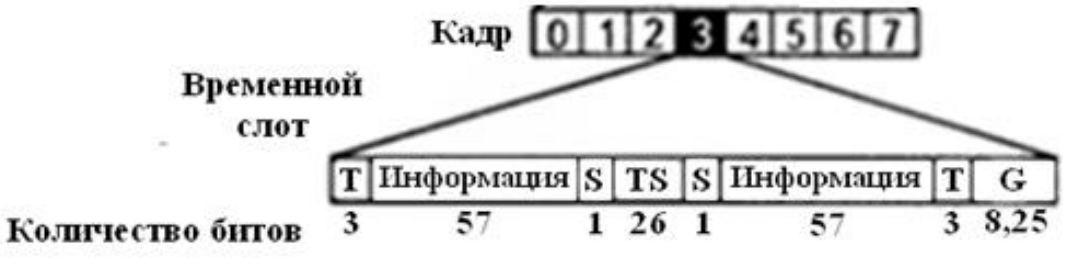



Рис. 2.5. Содержание информации во временном слоте

Длительность периода системных часов GSM обусловлена, в основном, применением алгоритма шифрования данных, использующего номер текущего кадра для генерирования ключа шифрования. Применение большого периода системных часов позволяет предотвратить несанкционированную расшифровку пользовательской информации и увеличивает уровень безопасности и конфиденциальности разговора.

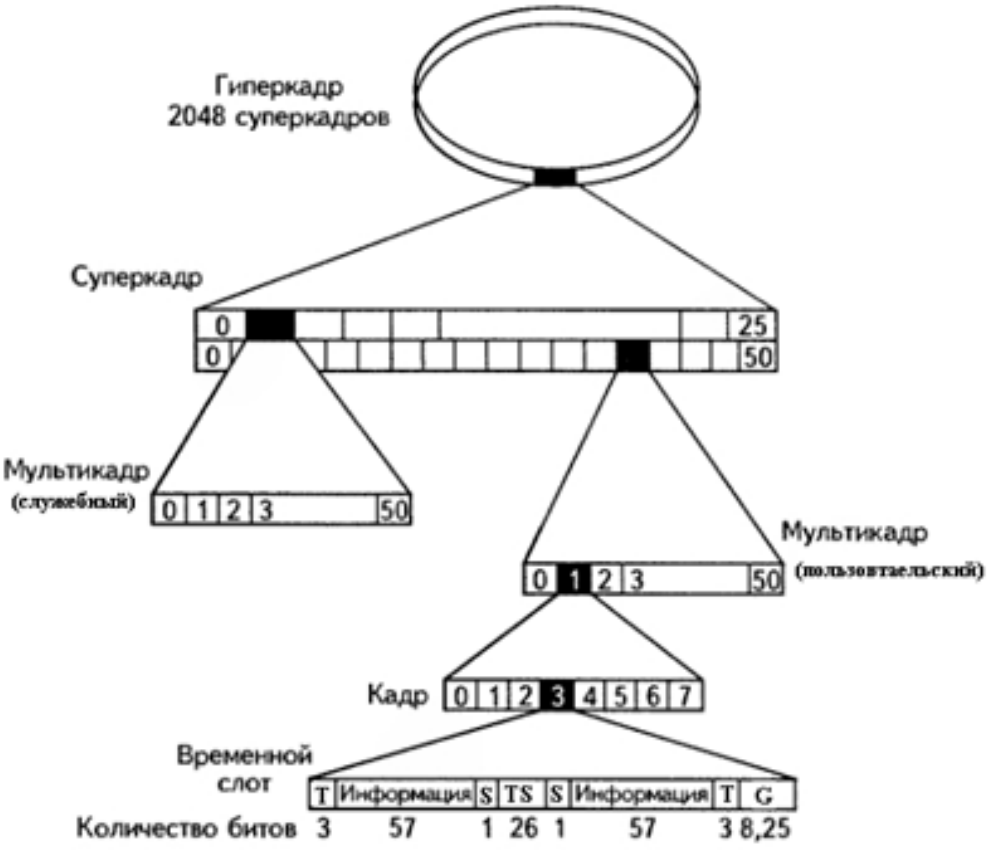



Рис. 2.6. Временная структура системы GSM

При рассмотрении систем организации сотовой связи считалось что, мобильные станции (МС) равномерно распределены во всей зоне охвата сотовой сети. На самом деле это крайне редкое явление. В реальных условиях имеет место неравномерное распределение МС в сотовой системе. Кроме того потребности абонентов изменяются как во времени, так и в пространстве. Решением этой проблемы является увеличение емкости системы. Емкость сотовой сети обычно увеличивается следующими методами:

## 2.3. Особенности построения мобильных сетей

1. *Разделение сот на секторы* - обычно соту разделяют на секторы по 120 градусов. При этом применяются секторные антенны;

2. *Дробление сот на минисоты* - выполняется путем создания сот меньшего размера в определенной части зоны покрытия соты. Радиусы минисот принимаются равными половине радиуса исходной соты, а их площади соответственно становятся меньше в четыре раза. Большие соты используются в районах с небольшим трафиком, а малые - в зонах с более интенсивным трафиком.

*Распределение каналов в сотах.* Рассмотрим правила распределения каналов среди сот и секторов. Непосредственное влияние на выбор оказывают межканальные помехи. Минимизировать искажения можно соответствующим подбором частот каналов в каждой соте. Межканальные помехи также тесно связаны с перемещением подвижных станций в границах одной соты и различными расстояниями от подвижных станций до общей базовой станции. Межканальные помехи существенно влияют на качество принимаемого полезного сигнала.

Все сигналы, поступающие с различных подвижных станций одной соты на базовую станцию этой же соты, должны иметь примерно одинаковую низкую мощность, обеспечивающую требуемое отношение "сигнал-помеха" для исключения вероятности появления ошибок. Все действующие сотовые системы применяют контроль мощности подвижных станций.

Если распределение каналов производится единожды и в последующем не меняется, то оно называется фиксированным распределением каналов. *Фиксированное распределение каналов* - простейший метод распределения ресурсов системы. При фиксированном распределении каналов установление нового

соединения в данной соте возможно только в том случае, если в ней есть незанятые каналы. В случае временного отсутствия доступных каналов абонент может столкнуться с блокировкой соединения. В этот момент в соседних сотах могут быть свободные каналы. Количество запросов может сильно меняться в зависимости от дня недели, времени суток или от конкретного события. Таким образом, фиксированное распределение каналов может оказаться неэффективным решением, приводящим к большой вероятности блокировки в часы наибольшей нагрузки. На рис. 2.7 представлена классификация стратегий распределения каналов.

*Метод простого заимствования каналов* представляет собой улучшенный вариант основной стратегии фиксированного распределения, к которой добавлено немного динамики. Если все каналы, выделенные конкретной соте, заняты, то свободный канал можно позаимствовать в соседней соте. С момента заимствования канала данной сотой, ряду окружающих сот запрещается использовать заимствованный канал во избежание межканальных и внутриканальных помех. Процессом заимствования управляет ЦКПС. Он блокирует заимствованные каналы в сотах, расположенных через одну или две соты от заимствующей соты. ЦКПС ведет базу данных свободных, заимствованных и блокированных каналов и информирует о них соответствующие базовые станции. Благодаря применению такой стратегии вероятность блокировки уменьшается до определенного порогового уровня, определяемого интенсивностью трафика.

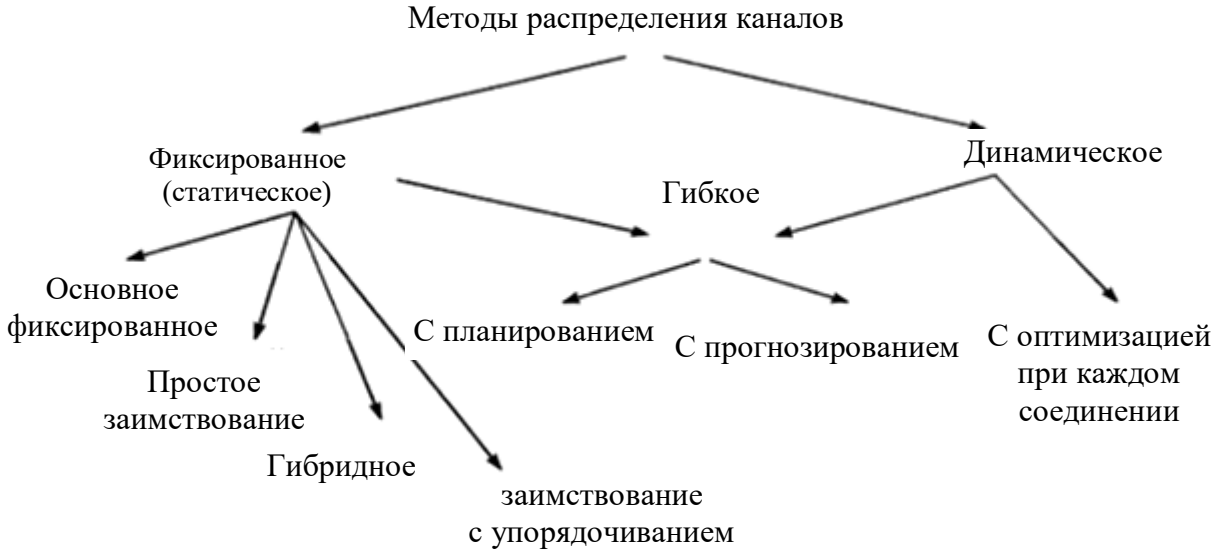



Рис. 2.7. Классификация распределения каналов

*Метод гибридного распределения каналов* устраняет недостатки предыдущего метода. В этом методе каналы в каждой соте делятся на две категории: в первую категорию входят каналы, используемые только в данной соте; ко второй относятся каналы, которые могут быть заимствованы. Соотношение количества каналов в обеих категориях определяется на основе ожидаемого трафика.

*Метод заимствования с упорядочиванием* - дальнейшее повышение коэффициента использования канала. При этом методе количество каналов, входящих в каждую категорию, динамически меняется в зависимости от объема трафика. Вероятность заимствования присваивается каждому каналу, подлежащему заимствованию. Каналы сортируются в порядке убывания этой вероятности. Значения вероятностей обновляются на основании данных о количестве заимствований каналов.

В *методе динамического распределения каналов* отсутствуют каналы, постоянно закрепленные за сотами. Каналы выделяются конкретному соединению или последовательно нескольким соединениям. Решение о выделении канала принимается либо центром коммутации, либо подвижной станцией. В первом случае речь идет о централизованном управлении; во втором - о распределенном управлении процессом выделения каналов.

*Метод гибкого распределения каналов* сочетает в себе преимущества фиксированного и динамического распределений. Каждая сота постоянно имеет в своем распоряжении набор каналов, достаточный для обслуживания трафика средней интенсивности. Центр коммутации управляет остальными каналами, которые могут быть выделены соте, испытывающей нехватку постоянных каналов для обслуживания высокого текущего трафика.

В стратегии *гибкого распределения каналов с планированием выделение дополнительных каналов* планируется заранее с учетом времени суток и расположения соты. Распределение каналов изменяется в заранее установленные моменты, предшествующие критическому возрастанию интенсивности трафика.

В стратегии *гибкого распределения каналов с прогнозированием* интенсивность трафика измеряется в режиме реального времени, и центр коммутации подвижной связи может перераспределить каналы в любой момент времени.

*Метод оптимизации параметров при соединении каналов* основан на определении стратегии распределения каналов, которая

должна оптимизировать некоторые параметры системы с учетом ограничения на повторное использование каналов.

Поиск канала для определенной соты в определенный момент времени включает в себя перебор всех каналов, выделенных для системы. Поиск свободного канала в данной соте может осуществляться некоторым регулярным образом среди всех выделенных каналов или по случайному закону. Если в наличии оказывается более одного канала, то выбор канала должен быть сделан в соответствии с некоторой стратегией оптимизации. Эта стратегия может быть основана на таких критериях, как порядок поиска, взвешенное расстояние для остальных сот, использующих тот же самый канал, число использований канала и т.п.

Результаты моделирования и анализа свидетельствуют, что при малой интенсивности трафика динамическое распределение каналов даст лучший результат, чем фиксированное. Однако фиксированное распределение показало свое превосходство в условиях больших объемов трафика и равномерного распределения подвижных станций по зоне охвата системы. При фиксированном распределении каналы выделяются таким образом, чтобы обеспечить их максимально многократное использование. Это невозможно осуществить в случае динамического распределения.

Приведенные методы распределения каналов дают всего лишь общее представление о многообразиях способов распределения каналов, представленных в специальной литературе.

Алгоритмы функционирования систем сотовой мобильной связи различных стандартов в основном схожи и характеризуются следующим.

1. Когда МС находится в режиме ожидания, ее приемное устройство постоянно сканирует либо все каналы системы, либо только управляющие каналы.

2. Для вызова абонента всеми БС фрагмента сети по каналам управления передаются сигналы вызова.

3. МС вызываемого абонента при получении сигнала вызова отвечает по одному из свободных каналов управления.

4. БС, принявшие ответный сигнал, передают информацию о его параметрах в центр коммутации ЦКПС, который переключает разговор на ту БС, где зафиксирован максимальный уровень сигнала МС вызываемого объекта.

5. Во время набора номера МС вызываемого абонента занимает один из свободных каналов БС, уровень сигнала которой в данный момент максимален.

6. По мере удаления вызываемого абонента от БС или в связи с ухудшением условий распространения радиоволн уровень сигнала уменьшается, что ведет к ухудшению качества связи. Улучшение качества разговора достигается путем автоматического переключения вызываемого абонента на другой канал радиосвязи.

## 2.4. Принципы построения мобильных сетей

Профессиональными системами мобильной или подвижной радиосвязи PMR (Professional Mobile Radio) называются телекоммуникационные системы, использующие в качестве каналов связи радиоканал и предусматривающие использование нестационарных (носимых) пользовательских терминалов (телефонов).

Как правило, они имеют радиальную или радиально-зоновую (сотовую) структуру сети и могут использовать как симплексные (односторонние), так и дуплексные каналы (двухсторонние) каналы связи. В связи с большим количеством различных по функциональному составу и назначению систем мобильной связи в международной трактовке для обобщенной классификации используется термин "система связи подвижной службы (ССПС)".

Система связи подвижной службы общего пользования является двухуровневой составной телекоммуникационной сетью, включающей систему мобильной радиосвязи (СМР) (первый уровень) и телефонную сеть общего пользования – ТСОП (англ. PSTN - Public Switched Telephone Network) (второй уровень). Двухуровневая телекоммуникационная сеть обеспечивает функции коммутации и распределения информации в каждой из составных частей (рис. 1.10).

Процессы распределения каналов в магистральных соединительных линиях рассматриваются как предоставление свободных линий связи для обслуживания транзитных разговоров между абонентами МС и абонентами сети ТСОП в требуемые моменты времени.

Таким образом, каналы ССПС являются составными каналами, объединяющими радиоуровень (СМР) и уровень фиксированной сети (ТСОП) телекоммуникационной системы.

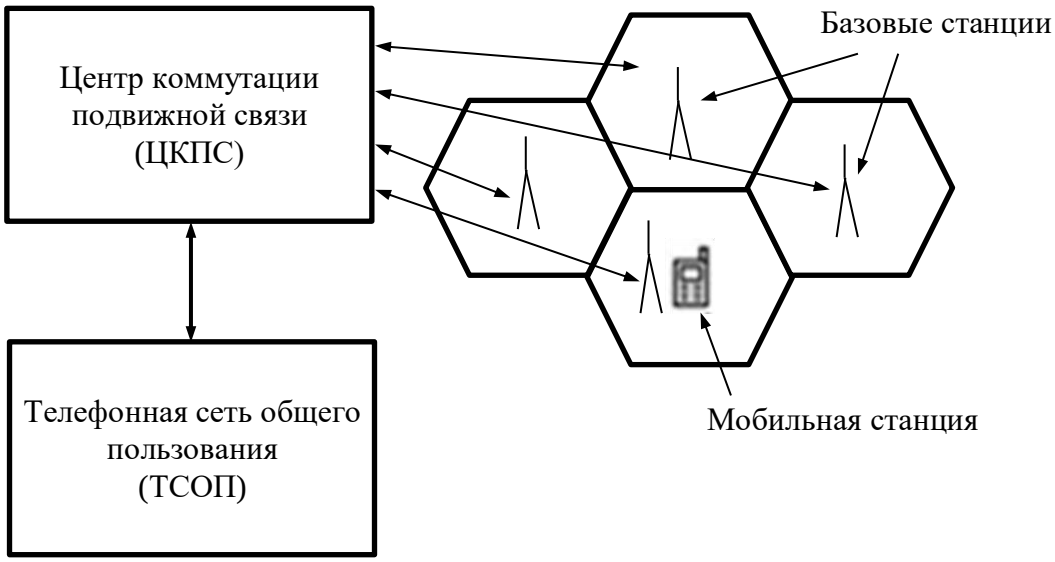



Рис. 2.8. Структурная схема сотовой системы подвижной радиосвязи

В настоящее время в различных странах мира применяются различные виды ССПС, которые обеспечивают информационные потребности экономики этих стран. Деление ССПС на виды определяется структурным построением радиоуровня (рис. 2.9).

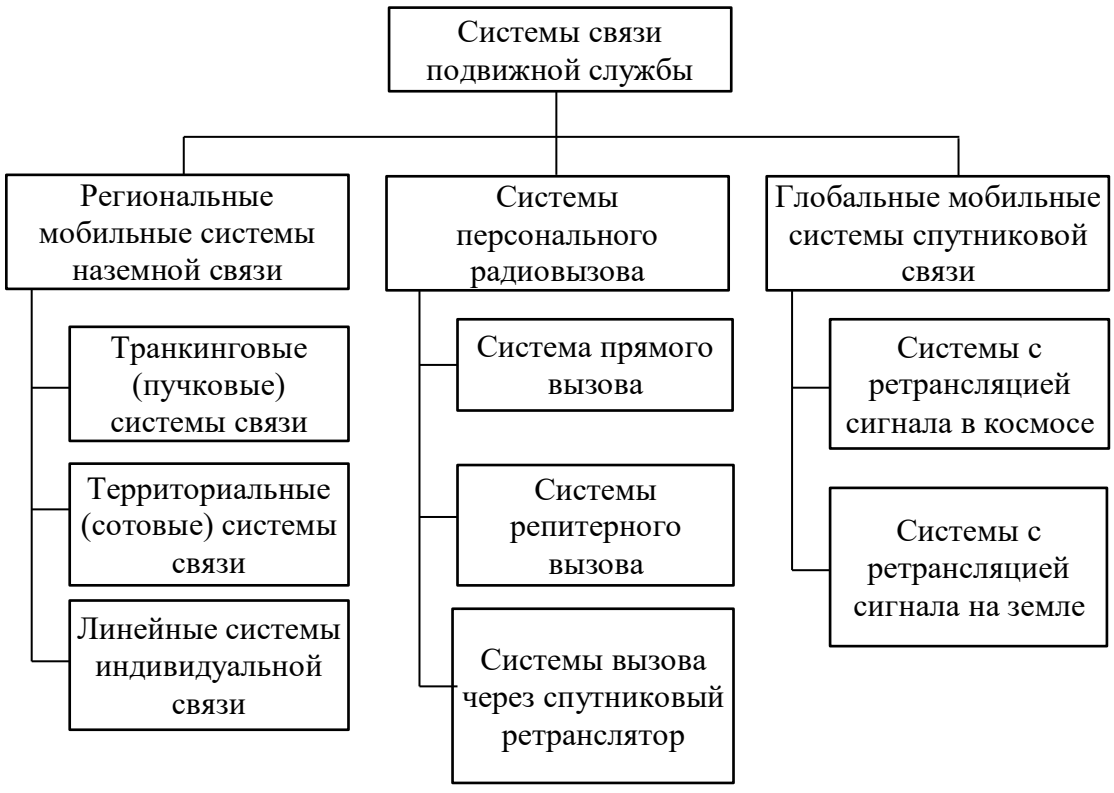



Рис. 2.9. Классификация систем связи подвижной службы

Система мобильной связи строится в виде совокупности ячеек (сот), покрывающих обслуживаемую территорию. Ячейки обычно схематически изображают в виде правильных шестиугольников. В центре каждой ячейки находится базовая станция БС, обслуживающая все мобильные станции МС в пределах своей ячейки. При перемещении абонента между ячейками системы происходит передача обслуживания от одной БС к другой - эстафетная передача (handover). Все БС соединены с центром коммутации (ЦКПС) подвижной связи по выделенным проводным или радиорелейным каналам связи. При перемещении абонента на территорию другой системы мобильной связи осуществляется передача его обслуживания от одной СМР к другой СМР - роуминг (roaming).

На рис. 2.10 приведена упрощенная функциональная схема мобильной сети.

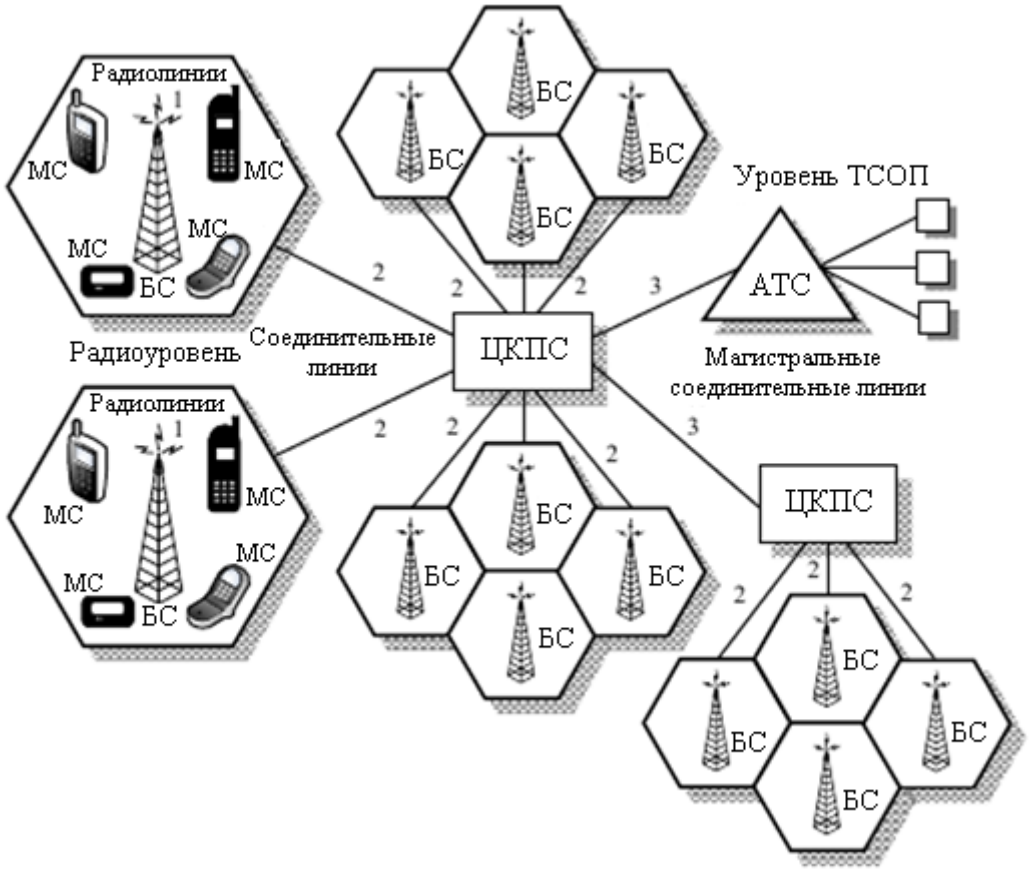



Рис. 2.10. Функциональная схема мобильной сети

Участки «1» составной сети являются радиолиниями, образованными между мобильными станциями (МС) и базовыми

станциями (БС). Участки «2» сети представляют многоканальные соединительные линии между БС и центром коммутации подвижной службы (ЦКПС). Участки «3» сети являются магистральными соединительными линиями (МСЛ) между радиоуровнем и телефонной сетью общего пользования (ТСОП). Множество базовых станций, размещаемых по всей зоне обслуживания системы, позволяет обеспечивать устойчивую радиосвязь любого мобильного абонента радиоуровня, в какой бы точке зоны обслуживания он не находился, с другим мобильным абонентом или с абонентом фиксированной сети ТСОП через центр коммутации подвижной связи (ЦКПС).

Таким образом, ЦКПС выполняет роль автоматического радиокросса, обеспечивающего коммутацию между собой различных мобильных станций в зоне обслуживания, коммутацию МС с абонентскими телефонными аппаратами сети, а также выход на ЦКПС других зон обслуживания.

# ГЛАВА 3. БЕСПРОВОДНЫЕ СЕТИ

## 3.1. Основные принципы построения беспроводных сетей

Известно, что вскоре после изобретения радио появилась возможность передачи телеграфной связи без проводов. И, по сути, сегодняшние системы передачи цифрового кода по радиоканалу используют тот же принцип, но, конечно, возможности передачи данных возросли многократно.

По радиусу действия и назначению современные беспроводные сети можно разделить на:

- персональные (Wireless Personal Area Network, WPAN);
- локальные (Wireless Local Area Network, WLAN);
- городские (Wireless Metropolitan Area Network, WMAN);
- глобальные (Wireless Wide Area Network, WWAN) (рис. 3.1).

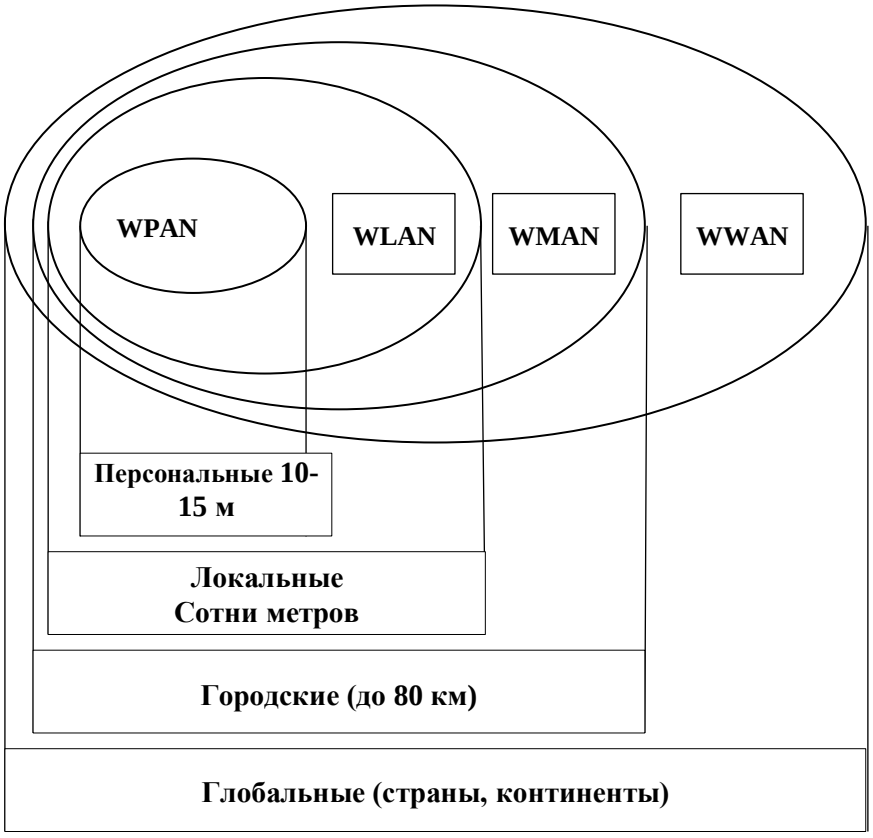



Рис. 3.1. Классификация беспроводных вычислительных сетей

Основные характеристики вышеперечисленных сетей представлены в табл. 3.1.

Таблица 3.1. Основные характеристики беспроводных сетей

| Беспроводные сети / Характе-ристики | **WPAN (персональные беспроводные сети)** | **WLAN (локальные беспроводные сети)** | **WMAN (городские беспроводные сети)** | **WWAN (глобальные беспроводные сети)** |
|---|---|---|---|---|
| Сфера применения | Замена проводов периферийных устройств | Мобильные расширения проводных сетей | Широкополосный беспроводной доступ | Мобильный доступ в Интернет вне помещений |
| Технологии | Bluetooth, UWB, ZigBee | Wi-Fi (802.11) | WiMax (802.16), MBWA-m (802.20) | GSM, GPRS, WCDMA, EDGE, HSPA+, WiMax, LTE |

*Беспроводные персональные сети (WPAN)* отличаются небольшим расстоянием передачи (до 17 метров) и используются в небольших зданиях. Характеристики таких сетей средние, и скорость передачи обычно не превышает 2 Мбит/с.

Такая сеть может обеспечить, например, беспроводную синхронизацию данных на персональном компьютере или ноутбуке. Таким же образом обеспечивается беспроводное соединение с принтером. Устранение путаницы проводов, соединяющих компьютер с внешними устройствами, является достаточно серьезным преимуществом, за счет которого первоначальная установка внешних устройств и последующее, при необходимости, смещение пространства становится заметно проще.

Дело в том, что большинство беспроводных персональных сетей потребляют меньше энергии, чем передатчик-приемник (трансивер), а ее портативность позволяет устройствам пользователей эффективно работать от батареи (или аккумулятора), что повышает производительность компьютерного устройства в течение длительного времени. Кроме того, низкое энергопотребление позволяет использовать беспроводные персональные сети для мобильных телефонов и наушников.

*Беспроводные локальные сети (WLAN)* обеспечивают высокие характеристики передачи внутри и вне офисов, в производственных зданиях. В таких сетях пользователи часто используют карманные персональные компьютеры (КПК), ноутбуки, персональные компьютеры и приложения, не требующие больших ресурсов. Беспроводные локальные сети имеют возможность соотвествовать

сфере применений офиса или домочадцев на скоростях передачи до 54 Mbit/s. По характеристикам, компонентам, цене и производительности такие сети аналогичны традиционным проводным локальным сетям Ethernet.

*Беспроводные городские сети (WMAN)* - это сети покрывающие площади городов. В большинстве случаев при выполнении приложений требуется определенное соединение, иногда и мобильное соединение. Например, такая сеть в больнице обеспечивает передачу данных между главным зданием и удаленными клиниками. Примером такой сети может сеть Sage desk (энергетическая сеть), которая распределяет наряды на работу районным филиалам из одного места, а также концентрирует в своей базе их выполнение. К этой сети могут подключаться пользователи со своих мобильных устройств.

Поставщики услуг беспроводного интернета (Wireless Internet Service Provider, WISP) предоставляют беспроводную сеть, как в городских, так и в сельских районах по усмотрению клиентов, обеспечивая непрерывное беспроводное соединение для домашних пользователей и компаний. Такие сети зачастую более эффективны, чем простые проводные соединения с прокладкой проводов. Характеристики беспроводных городских сетей разнообразны.

*Беспроводные глобальные сети (WWAN)* обеспечивают выполнение мобильных приложений с доступом, как по одной стране, так и имеет возможность межконтинентального охвата. Телекоммуникационные компании создают относительно дорогую инфраструктуру беспроводной глобальной сети, которая обеспечивает удаленное подключение для многих пользователей. Стоимость такого решения распределяется между всеми пользователями, в результате чего абонентская плата будет не очень высокой.

Благодаря сотрудничеству многих телекоммуникационных компаний, сфера влияния беспроводных глобальных сетей не ограничена. Через беспроводную глобальную сеть интернет-услугами можно пользоваться из любой точки мира, оплатив услуги одному из поставщиков телекоммуникационного сервиса.

Характеристики беспроводной глобальной сети не являются относительно высокими, скорость передачи данных составляет 56 Кбит/с, иногда 170 Кбит/с.

Приложения, специфичные для беспроводных глобальных сетей - это приложения, которые позволяют использовать Интернет, передачу и прием сообщений электронной почты. Как правило, пользователи беспроводной сети территориально не ограничены.

Беспроводные персональные, локальные, городские и глобальные сети дополняют друг друга и отвечают различным требованиям. При определении различий между беспроводными сетями используются применяемые в них различные технологии.

## 3.2. Технологии построения беспроводных сетей

***Беспроводные персональные сети.*** К категории беспроводных персональных сетей (WPAN) относится целый ряд технологий. Самой первой из технологий передачи данных в пределах малого радиуса действия является IrDA (Infrared Data Association) - технология передачи данных в инфракрасном диапазоне. Эта технология позволяет передавать данные в пределах свободного от препятствий пространства небольшого радиуса.

Более современной (и в настоящее время массовой) является технология Bluetooth. Для установления беспроводного соединения Bluetooth прямая видимость между устройствами не требуется, в отличие от инфракрасной связи. Перспективными являются технологии UWB (Ultrawideband) и ZigBee.

*Технология Bluetooth.* Радиосвязь Bluetooth осуществляется в диапазоне 2,4-2,48 ГГц. Спектр сигнала формируется по методу FHSS (Frequency Hopping Spread Spectrum) - широкополосный сигнал по методу частотных скачков, согласно которому несущая частота сигнала скачкообразно меняется 1600 раз в секунду. Последовательность переключения между частотами для каждого соединения известна только передатчику и приемнику, что позволяет обеспечить конфиденциальность передачи данных и исключить помехи, если рядом работают несколько пар "приемник-передатчик".

На базе универсального приемопередатчика обеспечивается связь с любыми Bluetooth-решениями, причем главным образом используются два варианта исполнения: либо Bluetooth-ключ (Bluetooth-dongle), либо подключаемые к специализированным материнским платам Bluetooth-адаптеры. На основе Bluetooth-технологии можно создать персональную беспроводную сеть.

На рис. 3.2 показано, что ноутбук с USB-ключом может взаимодействовать посредством беспроводной связи с мобильным телефоном, КПК и другими компьютерами. Bluetooth обеспечивает обмен информацией между такими устройствами, как ПК, ноутбуки, PDA, мобильные телефоны, принтеры и цифровые фотоаппараты, в радиусе от 10 до 100 м друг от друга и даже в разных помещениях.

Первое, с чего начинается работа Bluetooth-устройства в незнакомом окружении - это процедура device discovery, т.е. поиск других Bluetooth-устройств. Для этого посылается запрос, и ответ на него зависит не только от наличия в радиусе связи активных Bluetooth-устройств, но и от режима в котором находятся эти устройства.

На этом этапе возможно три основных режима:

1. *Discoverable mode.* Находящиеся в этом режиме устройства всегда отвечают на все полученные ими запросы.

2. *Limited discoverable mode.* В этом режиме находятся устройства, которые могут отвечать на запросы только ограниченное время, или должны отвечать только при соблюдении определённых условий.


Рис. 3.2. На базе универсального приемопередатчика Bluetooth-dongle обеспечивается связь с различными Bluetooth-устройствами

3. *Non-discoverable mode.* Находящиеся в этом режиме устройства, как видно из названия режима, не отвечают на новые запросы.

После всех процедур обнаружения, идентификации и первичных настроек, Bluetooth устройства могут перейти к обмену пользовательской информацией. Спецификация Bluetooth описывает пакетный способ передачи информации с временным мультиплексированием. В радиотракте применен метод FHSS. Исходя из принципов работы FHSS, вся полоса частот подразделена на определенное количество подканалов шириной в 1 МГц. Канал представляет собой псевдослучайную последовательность скачков по 79, 23 или 22 радиочастотным каналам. Каждый канал делится на временные сегменты продолжительностью 625 мкс, причем каждому сегменту соответствует определенная несущая частота (подканал). Передатчик перестраивается из одной несущей в другую синхронно с приемником. За секунду может происходить до 1600 частотных перестроек. Такое изменение частоты несущего также называется - hopping, а канала - hopping channel. Метод обеспечивает конфиденциальность и некоторую помехозащищенность передач. Последняя обусловлена тем, что если переданный по какому либо каналу пакет не был принят, то приемник сообщает об этом, и передача пакета повторяется на одном из следующих подканалов, уже на другой частоте.

При соединении одного Bluetooth устройства с несколькими другими, устройство которое обслуживает несколько соединений, называется *master* (или "ведущий"), а подключенные устройства - *slave* (или "ведомый"). К одному master может быть подключено до семи активных slave. Кроме активных slave (то есть, устройств, которые активно обмениваются данными), может существовать множество неактивных slave, которые не могут обмениваться данными с master, пока заняты все каналы, но, тем не менее, остаются, синхронизированы с ним. Такая структура называется piconet. Разные piconet не синхронизированы друг с другом по времени и частоте. Каждая из них использует свою последовательность частотных скачков. В пределах же одного piconet все устройства синхронизированы по времени и частоте. Для каждого *piconet* генерируется псевдослучайная последовательность скачков и определяется адресом его master устройства.

В одной piconet может быть только один master, однако каждый slave может одновременно являться master-ом для других устройств, и образовывать свой piconet. Несколько piconet объединенных таким образом образуют scatternet. В рамках scatternet разные устройства

могут не только быть одновременно master или slave для различных piconet, но и просто slave для разных piconet. Более наглядно с этой структурой можно ознакомиться на рис. 3.3.

Более того, в случае необходимости любой slave в piconet может стать master. Естественно, старый master при этом становится slave. Таким образом, в scatternet могут объединяться столько Bluetooth устройств, сколько необходимо, логические связи могут образовываться так, как это требуется, и могут изменяться как угодно, в случае необходимости.

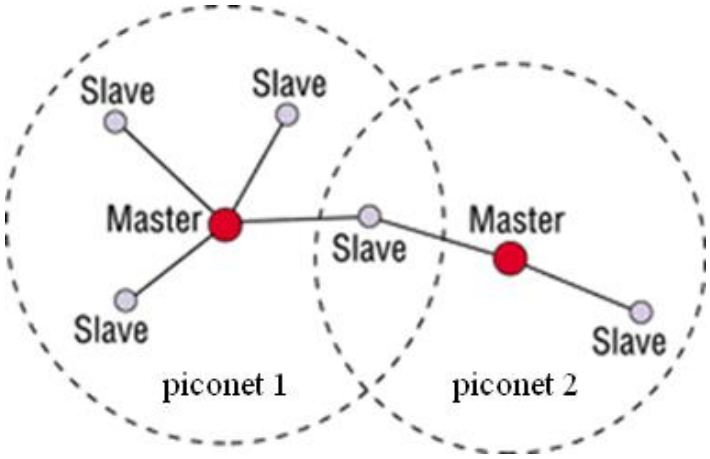



Рис. 3.3. Структура организации связи Bluetooth-устройств

В стандарте Bluetooth предусмотрена дуплексная передача на основе разделения времени - Time Division Duplexing (TDD). Master передает пакеты $f(k)$ в нечетные временные сегменты, а slave- в четные (рис. 3.4.). Пакеты в зависимости от длины могут занимать до пяти временных сегментов. При этом частота канала не меняется до окончания передачи пакета (рис.3.5).

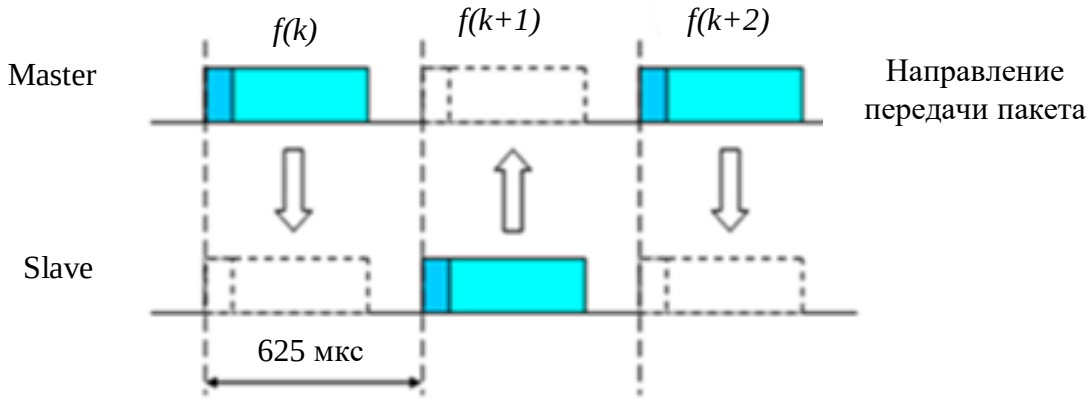



Рис. 3.4. Порядок передачи коротких пакетов

Протокол Bluetooth может поддерживать асинхронный канал данных, до трех синхронных голосовых каналов или канал с одновременной асинхронной передачей данных и синхронной передачей голоса.

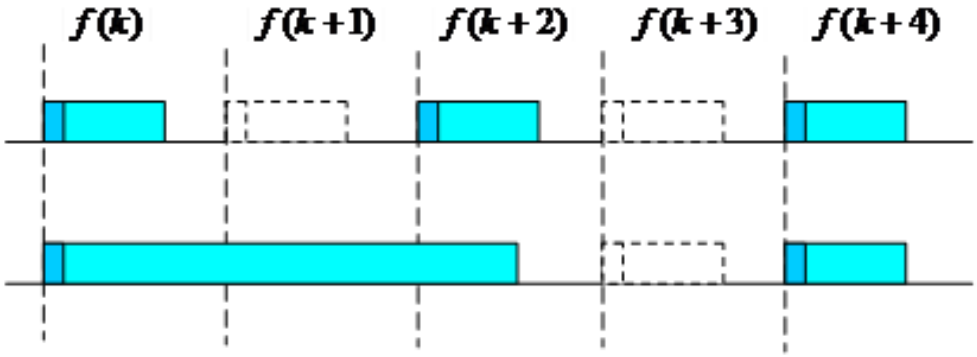



Рис. 3.5. Порядок передачи длинных пакетов

В настоящее время эта технология в основном используется в сенсорных системах, но ее сторонники считают, что технологию можно использовать для подключения дополнительных электронных устройств. В частности, компания Pantech-Curitel выпустила смартфон с интерфейсом ZigBee. Для управления "умными" домашними устройствами данной технологии сигнализация может использоваться в различных беспроводных средах (запыленность, шумность, влажность, перемещения и т.д.).

*Ultra wideband (UWB)*

В связи с расширением использования цифрового контента в персональных компьютерах, бытовой электронике и в мобильных коммуникационных устройствах появилась необходимость в едином стандартном средстве соединения, которое должно соответствовать наблюдающемуся сегодня процессу конвергенции в отношении указанных устройств. Постепенный переход к удобной беспроводной доставке цифровой информации создает предпосылки для создания единого и стандартизованного беспроводного средства подключения для разных областей применения.

Для устройств бытовой электроники необходим высокоскоростной беспроводной интерфейс, однако использование таких беспроводных технологий, как Bluetooth или других беспроводных протоколов имеет ряд ограничений. Основной недостаток этих протоколов заключается в их сравнительно небольшой полосе пропускания. Для доставки видео обычно требуется пропускная способность от 3 до 24 Мбит/с.

Альтернативной технологией беспроводного доступа, обеспечивающей обмен данными по радиоканалу между бытовыми электронными устройствами, периферийными устройствами ПК и мобильными устройствами на небольших расстояниях с очень высокой скоростью и малыми затратами энергии, является сверхширокополосная технология Ultra WideBand (UWB). Эта технология обладает высокой пропускной способностью при небольшом радиусе зоны покрытия и идеально подходит для беспроводной передачи высококачественного мультимедийного контента, в частности потокового цифрового видео от цифрового записывающего видеоустройства на телевизионное устройство стандарта ТВЧ (телевидение высокой четкости), или для беспроводного соединения мобильного ПК с проектором во время презентаций.

*Технология ZigBee*

ZigBee - беспроводная сетевая технология короткого радиуса действия, базирующаяся на стандарте IEEE 802.15.4. Данная технология была разработана с целью обеспечения более дешевого и менее энергоемкого решения по сравнению с другими WPAN-технологиями, в частности с Bluetooth. Протоколы ZigBee разработаны с учетом максимального энергосбережения: большую часть времени устройства находятся в спящем режиме и только изредка проверяют, поступили ли к ним обращения. Дальность связи между двумя аппаратами - до 75 м.

В настоящее время технология применяется в основном в сенсорных системах, но ее сторонники считают, что она может использоваться для соединения практически любых электронных устройств. В частности, фирма Pantech-Curitel уже выпустила смартфон с интерфейсом ZigBee. Ожидается, что данная технология будет применяться в разнообразных беспроводных средствах сигнализации (задымление, температура, шум, влажность, движение и т.п.), для управления устройствами "умного" дома.

***Технология локальной беспроводной сети (WLAN)*** основана на семействе стандартов 802.11. Технологии WLAN, принадлежащие к семейству стандартов 802.11, часто устанавливаются через термин Wi-Fi. В настоящее время этот термин используется в качестве альтернативы проводным локальным сетям со всеми данными, соответствующими необязательному стандарту в семействе 802.11.

Для домашней сети или небольшой офисной сети достаточно наличия одной точки использования, через которую осуществляется связь с оконечными устройствами сети через широкополосную связь с помощью коммутатора (рис.3.6).

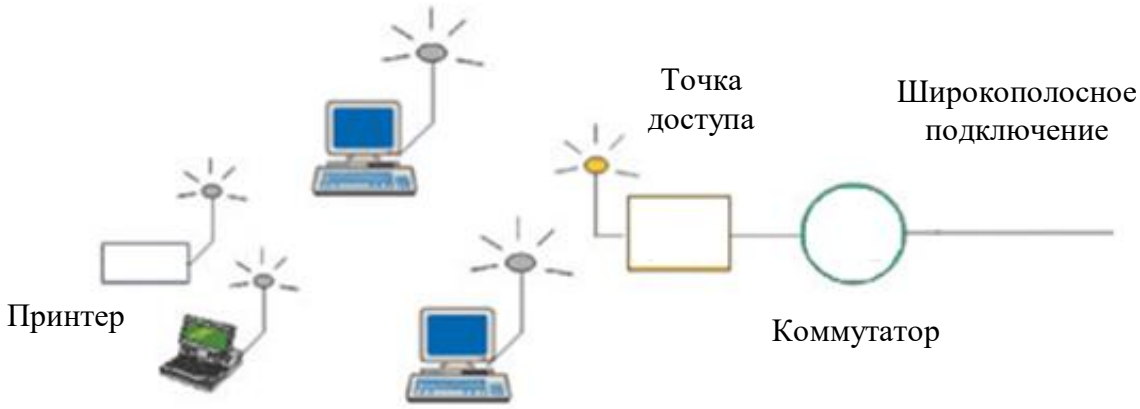



Рис. 3.6. Схема использования WLAN применительно к домашнему или малому офису

Для большого офиса одной точки подключения WLAN будет недостаточно. Из-за величины расстояний между последними Устройствам в сети офиса или организации установлено несколько точек доступа (рис. 3.7).

Помимо беспроводных домашних и офисных сетей, технология Wi-Fi широко используется в сфере организации массового использования Интернета.

Во многих аэропортах, отелях, ресторанах публичный доступ (платный или бесплатный) к Wi-Fi-сетям реализован посредством, так называемых хот-спотов. Каждый посетитель заведения, в котором есть хот-споты, получает возможность мобильного подключения к сети с помощью своего ноутбука, КПК или телефона, поддерживающего стандарт беспроводного доступа. В зависимости от конкретного стандарта сети Wi-Fi работают на частотах 2,4 или 5 ГГц и обеспечивают скорость передачи данных до 54 Мбит/с. Зону беспроводного доступа на базе нескольких хот-спотов называют хот-зоной (рис. 3.8).

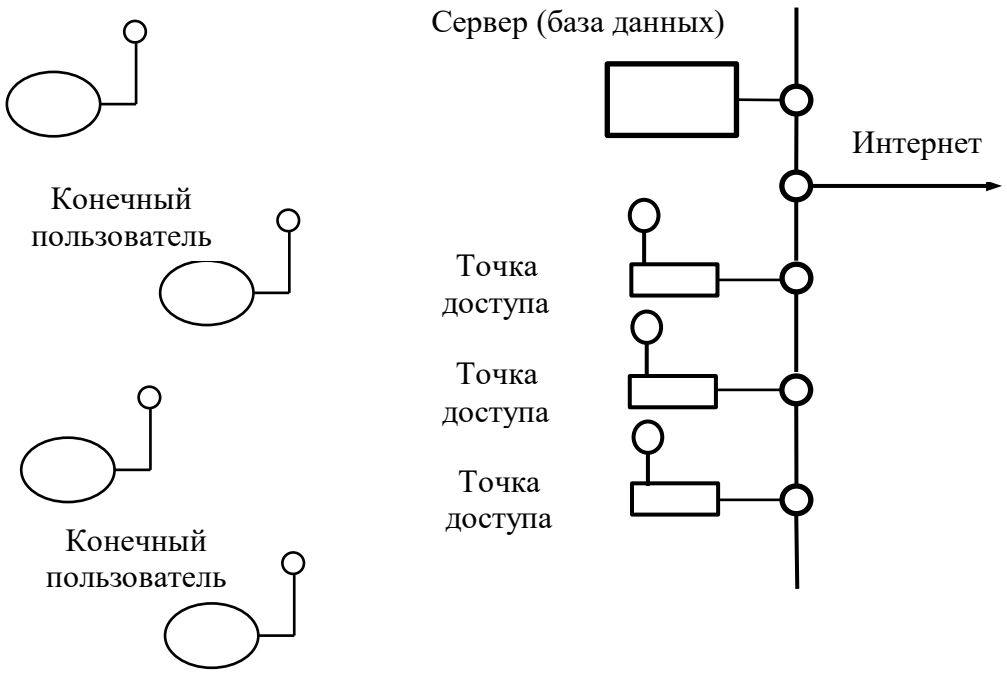



Рис. 3.7. Схема использования WLAN в крупном офисе

Радикальное увеличение пропускной способности дает стандарт 802.11n , с появлением которого пропускная способность WLAN будет увеличена сразу в несколько раз. Специалисты сходятся во мнении, что в ближайшее время технологию беспроводных сетей 802.11n станут поддерживать не только ноутбуки, но и многие бытовые электронные приборы и она будет использоваться всеми основными корпоративными и домашними приложениями.

В качестве перспективы развития беспроводных локальных и персональных сетей специалисты называют устройства Cognitive Radios, которые способны работать в разных диапазонах по различным протоколам, а также могут определять, в каком географическом районе они находятся и как там можно работать, подстраиваясь под местные требования.

***К городским беспроводным сетям (WMAN)*** относятся сети стандартов IEEE 802.16 (WiMAX) и 802.20 (Mobile Fi).

*Технология WiMAX.* WiMAX (Worldwide Interoperability for Microwave Access - международный стандарт для взаимодействия устройств микроволнового диапазона) - телекоммуникационная технология, разработанная с целью предоставления универсальной беспроводной связи на больших расстояниях для широкого спектра устройств (от компьютеров до мобильных телефонов). Работа

технологии основана на стандарте IEEE 802.16, который также называют Wireless MAN.

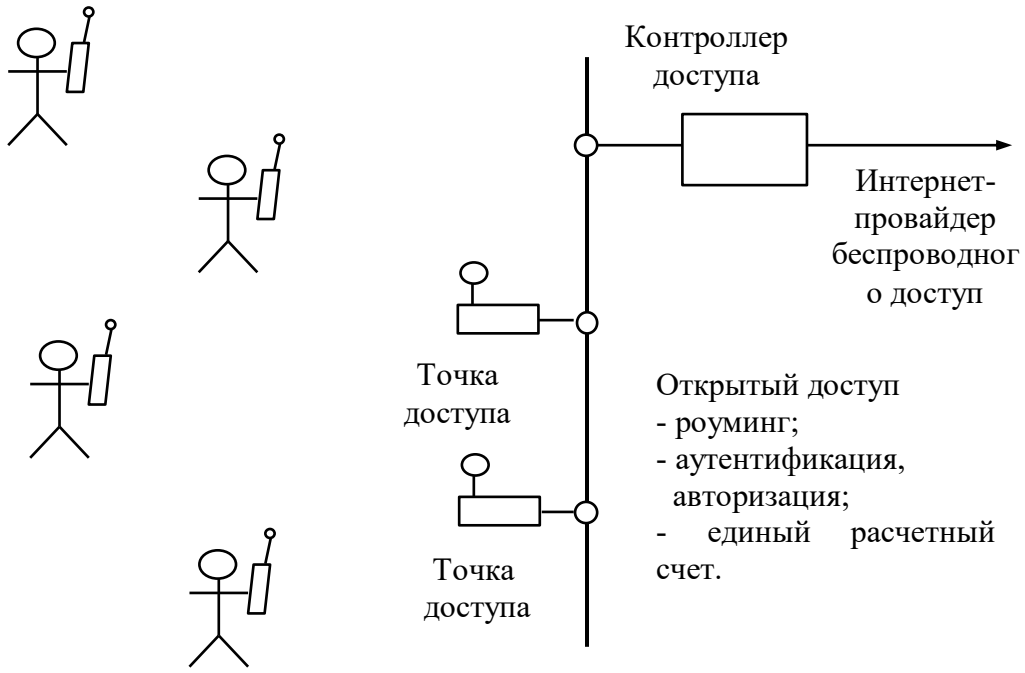



Рис. 3.8. Схема хот-спота

Технология WiMAX может быть использована для решения следующих задач:

- соединение точек доступа Wi-Fi друг с другом и другими сегментами Интернета;
- обеспечение беспроводного широкополосного доступа как альтернатива выделенным (проводным) линиям;
- предоставление высокоскоростных сервисов передачи данных и телекоммуникационных услуг;
- создания точек доступа, не привязанных к географическому положению.
- создания систем удалённого мониторинга (monitoring системы).

WiMAX позволяет осуществлять доступ в Интернет на высоких скоростях, с гораздо большим покрытием, чем у Wi-Fi-сетей. Это позволяет использовать технологию в качестве "магистральных каналов", продолжением которых выступают традиционные выделенные линии, а также локальные сети. В результате подобный подход позволяет создавать масштабируемые высокоскоростные сети в рамках городов.

В настоящее время известны 4 стандарта технологии WiMAX: 802.16a, 802.16d, 802.16e и 802.16f. Несмотря на одинаковую базу, эти четыре стандарта практически несовместимы.

Сеть WiMAX состоит из двух основных частей (рис. 3.9):

1. Базовая станция WiMAX, может размещаться на высотном объекте: здании или вышке;
2. Клиентский трансивер WiMAX - антенна с приёмником/передатчиком.

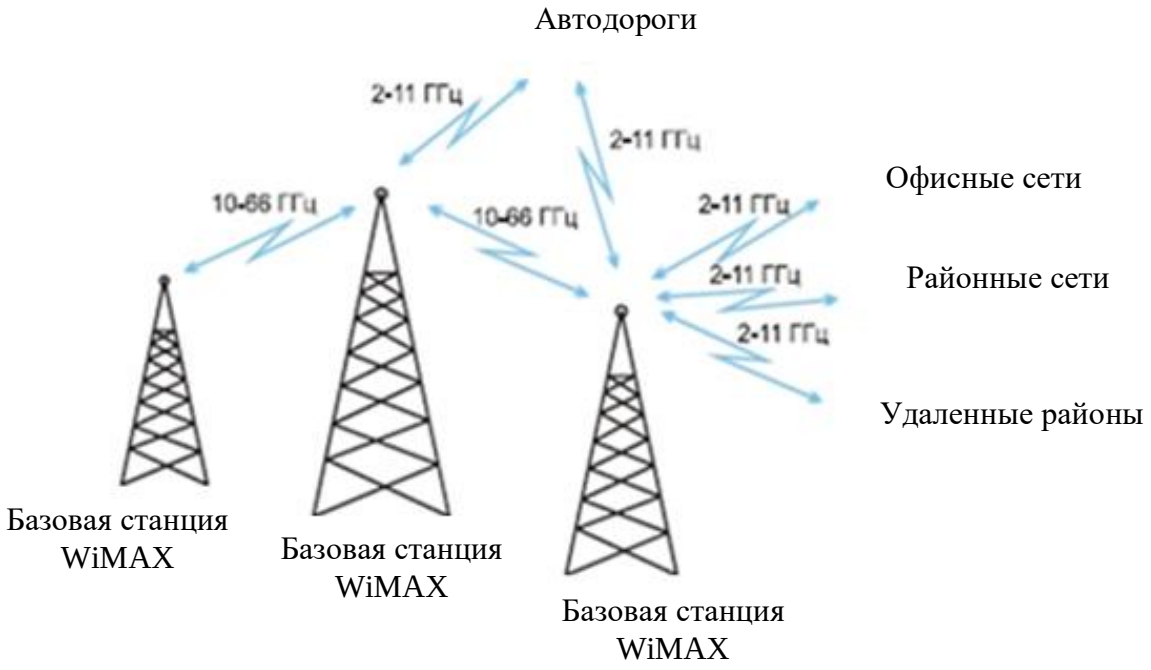



Рис.3.9. Структура сети WiMAX

Соединение между базовой станцией и клиентским трансивером производится в диапазоне 2-11 ГГц. Данное соединение позволяет передавать данные со скоростью до 20 Мбит/с и не требует наличия прямой видимости между станцией и пользователем. Этот режим работы базовой станции WiMAX близок широко используемому стандарту IEEE 802.11 (Wi-Fi), что допускает совместимость уже выпущенных клиентских устройств и WiMAX. Технология WiMAX применяется как на конечном участке между провайдером и пользователем, так и для предоставления доступа к региональным сетям: офисным, районным. Между соседними базовыми станциями устанавливается постоянное соединение с использованием диапазона частот 10-66 ГГц. Одна из базовых станций может быть постоянно связана с сетью провайдера через широкополосное скоростное соединение.

Типовая базовая станция имеет до 6 секторов. Структурная схема организации сети на основе стандарта 802.16 представлена на рис. 3.10.

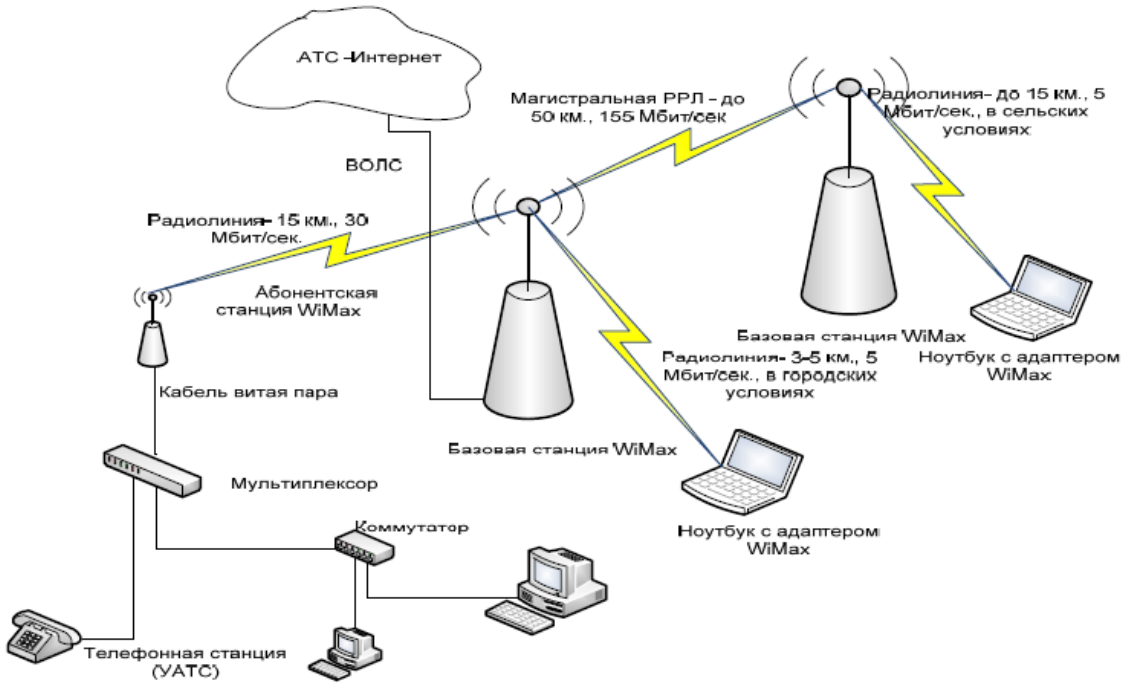



Рис. 3.10. Корпоративная сеть с фрагментами WiMax

По структуре сети WiMAX очень похожи на традиционные сети мобильной связи. Сигнал WiMAX может поступать по стандартному Ethernet-кабелю, как непосредственно на конкретный компьютер, так и на точку доступа стандарта Wi-Fi или в локальную проводную сеть стандарта Ethernet. Это позволяет сохранить существующую инфраструктуру районных или офисных локальных сетей при переходе с кабельного доступа на WiMAX.

На данный момент WiMAX технологии поддерживают следующие режимы работы:

- *Fixed WiMAX* - *фиксированный доступ* - представляет собой альтернативу широкополосным проводным технологиям. При этом все узлы сети остаются неподвижными.

- *Nomadic WiMAX* - *сеансовый доступ* - добавлено понятие сессий к уже существующему *Fixed WiMAX*. Наличие сессий позволяет свободно перемещать клиентское оборудование между сессиями и восстанавливать соединение уже с помощью других вышек WiMAX, нежели тех, что были использованы во время предыдущей сессии.

- *Portable WiMAX - доступ в режиме перемещения.* Для этого режима добавлена возможность автоматического переключения клиента от одной базовой станции WiMAX к другой без потери соединения. Скорость передвижения клиентского оборудования – до 40 км/ч.

- *Mobile WiMAX - мобильный доступ.* Этот режим позволяет увеличить скорость перемещения клиентского оборудования до 120 км/ч. Кроме того, режим устойчив к многолучевому распространению сигнала и собственным помехам без потери соединения при резкой смене направления движения клиентского оборудования и др.

Безопасность WiMAX-сети обеспечивается на физическом уровне специально разработанными чипами, которые встроены в устройства беспроводной связи и управляют процессом передачи данных по радиоканалу.

*Технология MBWA-m 802.20.* IEEE 802.20 или Мобильный широкополосный беспроводной доступ (англ. Mobile Broadband Wireless Access, MBWA) – стандарт создан для мобильного беспроводного доступа к сетям Интернет. В отличие от WiMax, рассчитанного на работу в городах при ограниченном числе базовых станций, 802.20 имеет больше сходства с обычными сотовыми системами и предназначен для быстродействующих мобильных подключений на скоростях свыше 1 Мбит/с в 3-ГГц частотном диапазоне. Данный стандарт занимает интересное положение среди остальных стандартов – с одной стороны, его называют ближайшим конкурентом WiMAX (802.16e), с другой стороны, он может использоваться в системах сотовой связи, заменяя GPRS или CDMA2000, а это уже WWAN. Технология обеспечивает работу и при перемещении абонентских терминалов на больших скоростях (до 250 км/час) вне зоны прямой видимости.

Радиус соты MBWA может достигать 15 км. Ширина полосы радиоканала - от 1.25 МГц до 40 МГц.

***Глобальные беспроводные сети (WWAN).*** Стандарты сетей WWAN принято делить на поколения. К первому (The 1st Generation, 1G) относятся аналоговые стандарты, которые постепенно ушли в прошлое. Говоря о втором поколении (2 G), прежде всего, следует сказать о GSM (Global Standard for Mobile Communications) - глобальном стандарте для мобильной сотовой связи с разделением канала по принципу TDMA. В сотовых цифровых сетях стандарта

GSM может передаваться не только оцифрованная речь, но и цифровые данные.

Абоненты сетей GSM могут пользоваться услугами мобильного модема, получать доступ к компьютерным системам их офисов, посылать и принимать сообщения электронной почты. Одним из основных недостатков таких сетей является низкая скорость передачи.

Возможности мобильного доступа в Интернет были значительно расширены с переходом на использование технологии GPRS (General Packet Radio Service - пакетная передача данных по радиосетям) - надстройка над технологией мобильной связи GSM, осуществляющая пакетную передачу данных. Теоретический максимум скорости передачи данных составляет 171,2 Кбит/с (зависит от класса GPRS).

Дальнейшим развитием технологии CDMA является WCDMA (Wideband Code Division Multiple Access) - широкополосный множественный доступ с кодовым разделением - технология радиоинтерфейса, использующая широкополосный множественный доступ с кодовым разделением каналов, использующий две широкие полосы радиочастот по 5 МГц.

Следующий этап в развитии технологий мобильного доступа это технология EDGE (англ. Enhanced Data rates for GSM Evolution) - цифровая технология беспроводной передачи данных для мобильной связи, которая представлявляет собой надстройку над GPRS сетями.

Подключение в сети по EDGE примерно в 3 раза быстрее, чем по GPRS, а именно максимальная скорость передачи данных может составлять 474 Кбит/с.

Радикальное увеличение произошло в высокопроизводительных сотовых сетях третьего поколения (3G).

Из разновидностей 3G технологий в настоящее время используются:

*Технология HSPA*

Максимальная теоретическая скорость передачи данных по стандарту HSPA составляет 14,4 Мбит/с (скорость передачи данных от базовой станции на всех локальных абонентов) и до 5,76 Мбит/с от абонента. Первые этапы внедрения стандарта имели скорость 3,6 Мбит/с к абоненту HSDPA (D — downlink). После внедрения второго этапа HSUPA (U — uplink, то есть ускорения передачи от абонента) всю технологию сокращённо стали называть HSPA.

*Технология HSPA+*

HSPA+ (англ. Evolved High-Speed Packet Access, "развитый высокоскоростной пакетный доступ") — стандарт мобильной связи, модернизация третьего поколения мобильной связи, с высокой скоростью, сравнимой с 4G. К HSPA+ принято относить технологии, позволяющие осуществлять пакетную передачу данных со скоростью скачивания до 42,2 Мбит/с и отдачи до 5,76 Мбит/с. На практике скорость соединения ниже и составляет 10 — 20 Мбит/с.

Эта технология считается переходной между сетями третьего (3G) и четвёртого (4G) поколения. Иногда её ещё называют "3.5G".

*Технологии четвертого поколения беспроводных сетей (4G).*

Технологии WiMAX и LTE (Long-Term Evolution) считаются технологиями четвертого поколения, но это верно лишь отчасти - они оба используют новые, чрезвычайно эффективные схемы мультиплексирования (OFDMA, в отличие от старых CDMA или TDMA которые мы использовали на протяжении последних двадцати лет) и в них обоих отсутствует канал для передачи голоса.

*Технологии L, LTE, LTE-A*

В стандарте установлено 173 Мбит/с от сети к абоненту и 58 Мбит/с от абонента к сети.

Системы связи 4G основаны на пакетных протоколах передачи данных. Для пересылки данных используется протокол IPv4; в будущем планируется поддержка IPv6.

С технической точки зрения, основное отличие сетей четвёртого поколения от третьего заключается в том, что технология 4G полностью основана на протоколах пакетной передачи данных, в то время как 3G соединяет в себе как пакетную коммутацию, так и коммутацию каналов. Для передачи голоса в 4G предусмотрены технологии VoLTE (Voice over LTE).

Основные исследования при создании систем связи четвёртого поколения ведутся в направлении использования технологии ортогонального частотного уплотнения OFDM. Кроме того, для максимальной скорости передачи используется технология передачи данных MIMO (Multiple Input Multiple Output). MIMO - метод пространственного кодирования сигнала, позволяющий увеличить полосу пропускания канала, в котором передача данных и прием данных осуществляются системами из нескольких антенн. Передающие и приёмные антенны разносят так, чтобы корреляция между соседними антеннами была слабой.

# ГЛАВА 4. СИСТЕМЫ МОБИЛЬНОЙ СПУТНИКОВОЙ СВЯЗИ

## 4.1. Общие принципы построения мобильной спутниковой связи

Системы мобильной спутниковой связи представляют сравнительно новый, очень мощный, гибкий и быстро развивающийся вид мобильной связи. Использование спутников в системах связи началось фактически сразу же после запуска первых искусственных спутников Земли (ИСЗ).

В настоящее время представляются актуальными следующие области применения мобильной спутниковой связи:

- расширение сотовых сетей (cellular extension): использование спутниковой связи вместо сотовой в тех районах, где последней пока нет или ее развертывание нецелесообразно, например, из-за низкой плотности населения;

- дополнение сотовых сетей (cellular complement): использование спутниковой связи в дополнение существующей сотовой, например, для обеспечения роуминга при несовместимости стандартов или в каких-либо чрезвычайных ситуациях;

- стационарная беспроводная связь (fixed wireless), например, в малонаселенных районах при отсутствии проводной связи.

Тем самым спутниковая связь не выступает в качестве конкурента сотовой связи, а достаточно органично сочетается с последней. Практически во всех системах мобильной спутниковой связи предусматривается довольно высокая степень интеграции с сотовой связью. В частности, помимо абонентских терминалов, предназначенных для спутниковых систем, предполагается создание двухрежимных терминалов, предназначенных для работы, как в спутниковой системе, так и в каком либо из сотовых стандартов.

Как же осуществлялась радиосвязь на большие расстояния в период до спутниковой эпохи? Особенно, когда по экономическим и техническим причинам проводная связь на большие расстояния была невыгодной или трудно осуществимой. В этих случаях дальняя связь осуществлялась с помощью радиорелейных систем.

Линия радиосвязи может состоять из нескольких или многих отрезков, в пределах которых передача радиосигналов обеспечивается комплектами приемно-передающего оборудования. Сигналы из одного пункта принимаются в другом, усиливаются и передаются далее в третий пункт, там вновь усиливаются и

передаются в четвертый пункт и т.д. Такое построение радиолинии и называется радиорелейной линией связи (РРЛ) (рис. 4.1), а условное изображение приведено на рис. 4.2.

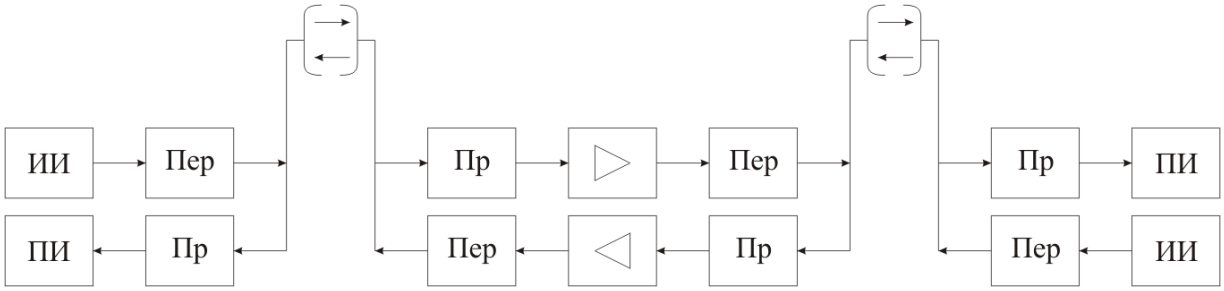



Рис. 4.1. Структурная схема радиорелейной линии связи

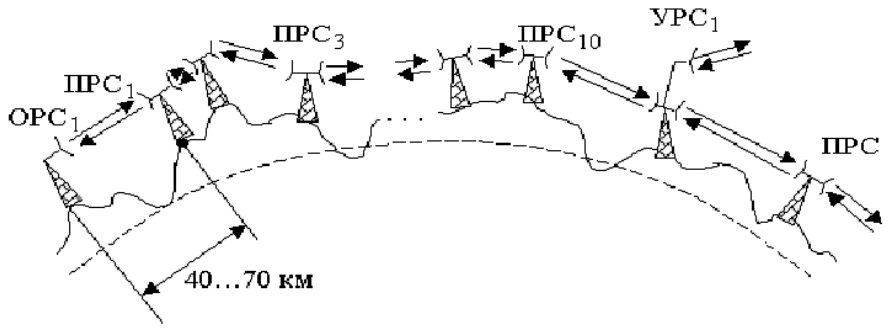



Рис. 4.2. Схематичное представление радиорелейной линии

Как действует спутниковая связь? Сигнал с одной наземной станции принимается на ИСЗ, усиливается и через передатчик спутника передается на другую наземную станцию, находящуюся на большом расстоянии от первой (рис. 4.3).

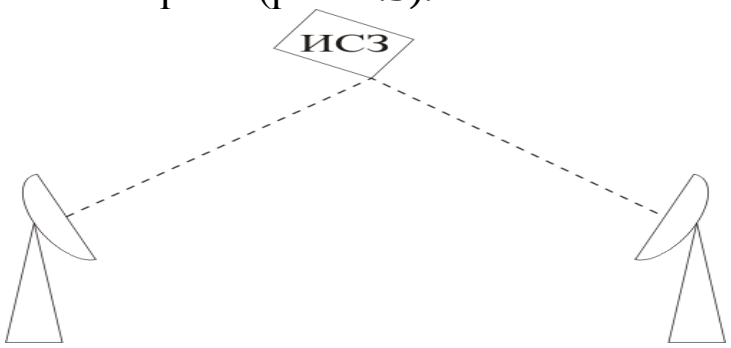



Рис. 4.3. Спутниковая линия связи

Принцип действия систем спутниковой связи (ССС) основан на использовании промежуточного спутникового ретранслятора (СР), через который обеспечивается связь между земными станциями (ЗС) (рис. 4.4).

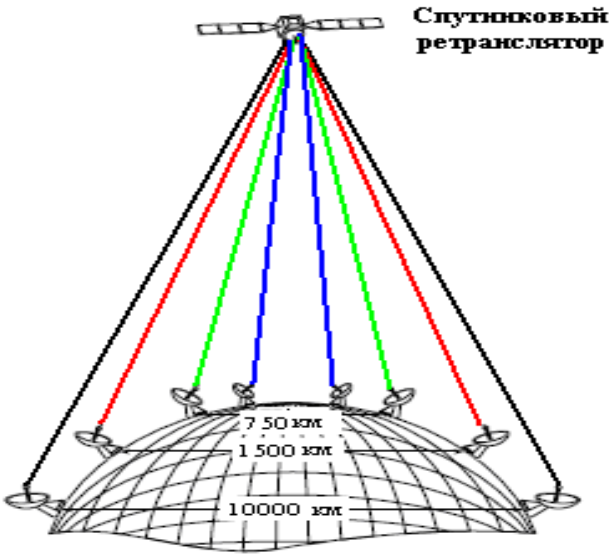



Рис. 4.4. Обеспечение связи между земными станциями через спутниковый ретранслятор

В зависимости от назначения системы спутниковой связи связывают пункты, которые могут быть расположены на поверхности Земли, в атмосфере или космосе. В каждом из этих пунктов устанавливается обычно приемно-передающая связная радиостанция (одноканальная или многоканальная), а на спутниках – спутниковый ретранслятор, принимающие радиосигналы от одних абонентов и ретранслирующие эти сигналы другим абонентам. В простейшем случае ретрансляция сводится к усилению мощности входных сигналов и переносу их спектров на другие несущие частоты. Однако в ряде систем спутниковой связи в спутниковых ретрансляторах производится более сложная обработка сигналов, чтобы уменьшить перекрестные помехи между сигналами от различных систем спутниковой связи и повысить помехоустойчивость системы. В общем случае для обеспечения качественной связи между всеми пунктами (абонентами) спутниковые ретрансляторы приходится размещать на нескольких спутниках вращающихся на различных орбитах.

Системы спутниковой связи различают по степени глобальности и универсальности обслуживания абонентов. Степень глобальности таких систем характеризуется принадлежностью и размером зоны обслуживания, а универсальность систем спутниковой связи - набором категорий абонентов и числом видов предоставляемой связи.

По принадлежности системы спутниковой связи подразделяются на международные, национальные, корпоративные. По зоне обслуживания системы спутниковой связи делятся на глобальные, региональные, зональные.

В системах спутниковой связи осуществляется передача следующих видов информации:

- программ телевидения и звукового вещания и других видов симплексных сообщений циркулярного характера;
- телефонных, факсимильных, телеграфных сообщений, видеоконференций.

В зависимости от типа земной станции и назначения спутниковой системы связи различают следующие службы радиосвязи:

- фиксированную спутниковую службу - соответствующую режиму радиосвязи между земными станциями, расположенных в фиксированных пунктах при использовании одного или нескольких спутников;
- подвижную спутниковую службу - соответствующую режиму радиосвязи между подвижными земными станциями при использовании одного или нескольких спутников;
- радиовещательную спутниковую службу, соответствующую режиму циркулярной радиосвязи.

## 4.2. Состав и основные характеристики мобильной спутниковой связи

В состав систем спутниковой связи с подвижными объектами, структура которой приведена на рис. 4.5, входят такие компоненты, как:

- космическая станция (КС) - представляющая собой спутниковый ретранслятор (СР), включающая в себя приемопередающее устройство, антенны для приема и передачи радиосигналов, а также ряд систем обеспечения энергоснабжения,

ориентации антенн и солнечных батарей, коррекции положения искусственного спутника Земли на орбите и т.д.;

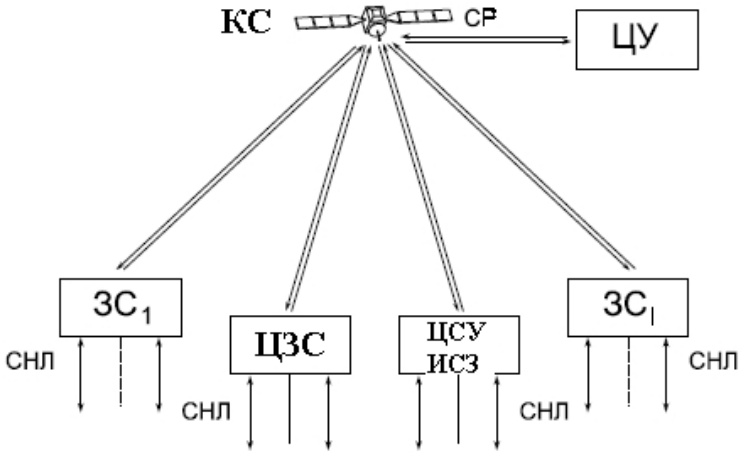



Рис. 4.5. Структура спутниковой связи с подвижными объектами

- абонентские земные станции - обеспечивающие дуплексный обмен информацией;

- центральная (координирующая) земная станция (ЦЗС) - обеспечивающая контроль за режимом работы спутникового ретранслятора и соблюдением важных для работы системы спутниковой связи параметров земных станций (излучаемой мощности, несущей частоты, вида поляризации характеристик модулирующего сигнала и т.д.);

- центральная система управления искусственным спутником Земли (ЦСУ ИСЗ) - обеспечивающая управление всеми техническими средствами, размещенными на ИСЗ и контроль за их состоянием;

- соединительные наземные линии (СНЛ) - обеспечивающие подключение земной станции к источникам и потребителям передаваемой информации;

- центр управления систем спутниковой связи (ЦУ ССС) - представляющий орган, осуществляющий руководство эксплуатацией ССС и ее развитием.

Существующие и разрабатываемые системы спутниковой связи с подвижными объектами в зависимости от высоты орбиты используемых в них искусственных спутников Земли можно подразделить на геостационарные, системы спутниковой связи на

эллиптических орбитах и низкоорбитальные системы спутниковой связи (рис. 4.6).

Использование в системах спутниковой связи геостационарных орбит обеспечивает следующие достоинства:


Рис. 4.6. Типы орбит в системах спутниковой связи

- связь осуществляется непрерывно, круглосуточно, без переходов с одного искусственного спутника Земли на другой и без необходимости отслеживания антеннами положения спутника;
- обеспечивается постоянное значение ослабления сигнала на трассе между земной станцией и спутниковым ретранслятором, поскольку расстояние имеет стабильное значение;
- практически отсутствует доплеровский сдвиг частоты сигнала излучаемого искусственным спутником Земли;
- зона видимости геостационарного спутника - около трети земной поверхности, что обуславливает возможность создания глобальной системы связи при использовании трех спутников (рис. 4.7).

Благодаря указанным преимуществам геостационарную орбиту используют очень широко. В настоящее время геостационарная орбита насыщена спутниками связи уже почти до предела. Причем наибольшая насыщенность создается спутниками, относящимися к фиксированной и отчасти радиовещательной службам. В настоящее

время на геостационарной орбите находится более 300 искусственных спутников Земли различных стран (при максимально возможном их числе около 360). Если учесть, что не все позиции удобны для размещения спутников в конкретных системах спутниковой связи, становится ясно, что наращивание емкости орбиты за счет увеличения числа спутников не даст заметных результатов. Более полному использованию ресурсов геостационарной орбиты способствует дальнейшее развитие систем спутниковой связи на геостационарных орбитах путем многократного повторения рабочих частот, а также освоения более высокочастотных диапазонов.

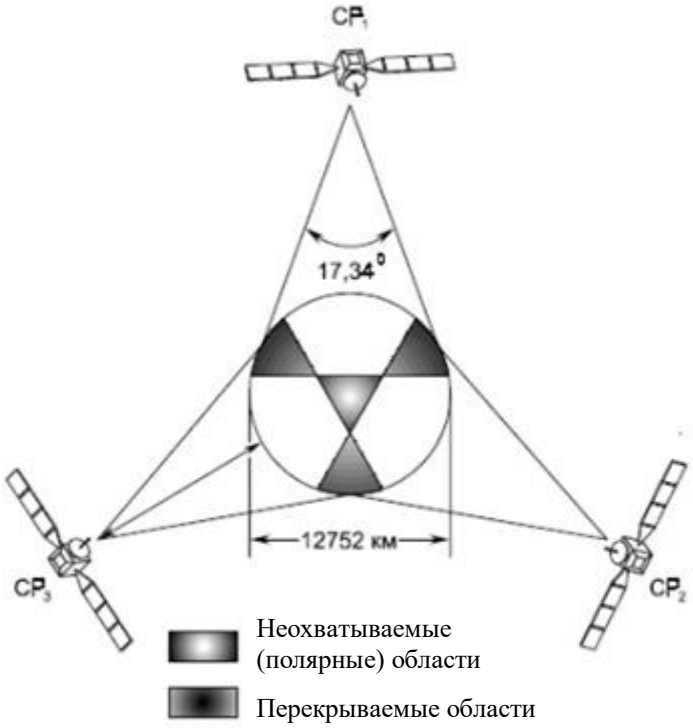



Рис. 4.7. Схема охвата Земли тремя геостационарными спутниками

Спутниковый Интернет, как правило, использует так называемую геостационарную орбиту. Основная задача спутника Земли на этой орбите, является передача информации из одной точки планеты (от базовой станции) для абонентов, когда спутник Земли находится в зоне спутника Земли (это очень большая территория, как правило, содержит несколько стран). Схема организации спутникового интернета Земли представлена на рисунке 4.7.

Основным преимуществом данной технологии является зона покрытия. Одна зона покрытия базовой станции сотового оператора

покроет территорию, равную одному кварталу или микрорайону. Тем не менее, данные передаются всем пользователям одновременно. Абонент должен идентифицировать свою собственную электромагнитную волну (несущую волну), чтобы использовать определенный канал данных.

Параметры этой несущей предоставляет провайдер спутникового Интернета. И они включают в себя:

- частоту несущей (МГц);
- символьную скорость (кбит/с);
- тип поляризации электромагнитной волны (правая/левая, вертикальная/горизонтальная).

Кроме того, на одной несущей волне, как правило, присутствуют данные нескольких пользователей. Для их идентификации используются специальные идентификаторы (PID, LID) и MAC адрес карты приемной карты (ресивера).

Также для организации более надежного соединения используются специальные программы (акселераторы), которые помимо шифрования трафика, еще и сжимают его, что экономит частотный ресурс спутника и способствует увеличению скорости передачи данных.

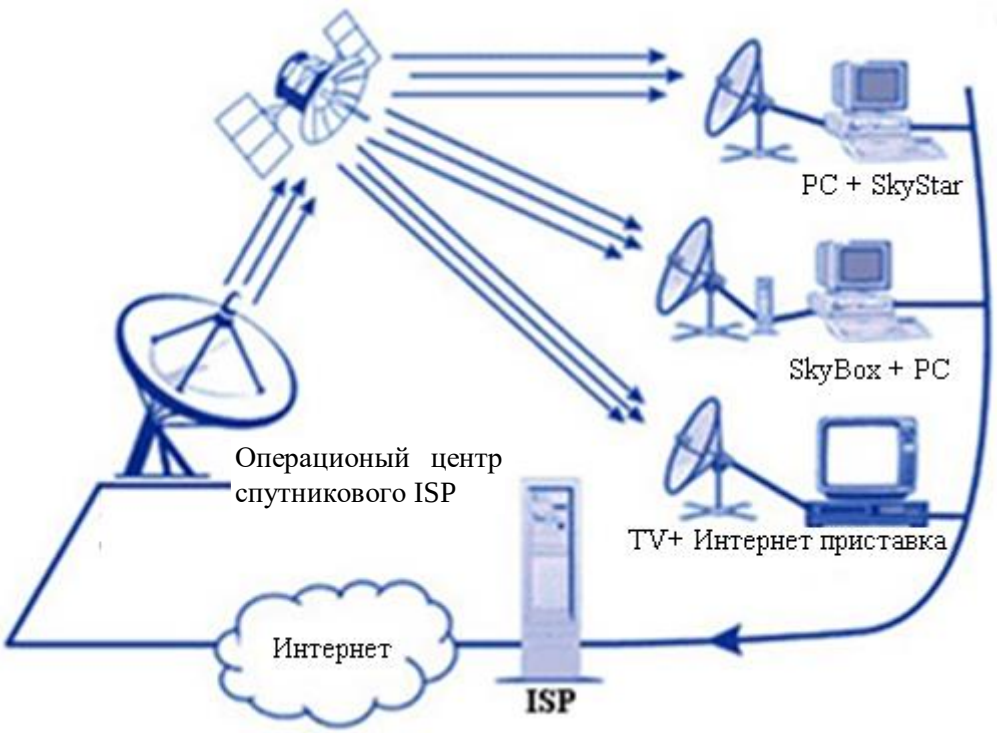



Рис. 4.7. Схема организации спутникового Интернета

Специалисты выделяют два типа подключения к спутниковому Интернету: симметричный и асимметричный. Такое различие в первую очередь связанно с организацией входящих (из Интернета) и исходящих (передача в Интернет) каналов передачи трафика.

*1. Симметричный доступ* в Интернет подразумевает, что данные со спутника и на спутник передаются с помощью одной антенны и двух (или одного) передатчика. Из-за высокой стоимости данный тип подключения не пользуется популярностью у рядовых пользователей.

*2. Асимметричный доступ* в Интернет в этом смысле намного доступнее в силу свой экономичности. Он подразумевает использование только входящего соединения через спутник (т.е. для антенны требуется только дешевый приемник), а исходящее соединение организуется через любой наземный канал связи.

Эффективность данного типа соединения объясняется тем, что пользователь чаще всего использует Интернет для скачивания медиа контента, просмотра почтовых сообщений или посещения социальных сетей. Т.е. рядовой пользователь чаще всего посылает короткие запросы в Интернет, а из Интернета скачивает большие объемы данных.

# ГЛАВА 5. УГРОЗЫ БЕЗОПАСНОСТИ В МОБИЛЬНЫХ СИСТЕМАХ

## 5.1. Классификация угроз безопасности информации в мобильных системах

Когда мы говорим об угрозах безопасности под этим понимается действие или событие, которое может привести к нарушениям, изменениям или несанкционированному использованию сетевых ресурсов, включая защиту, передачу и обработку информации, а также программного и аппаратного обеспечения.

Принято делить угрозы на случайные (неосознанно) и преднамеренные, т.е. сделаны сознательно. Ошибки в программном обеспечении, отказ аппаратных средств массовой информации, неправильное поведение потребителя или администрации сети, все это может быть источником случайных угроз. Угроза осуществленная преднамеренно, фокусирует свою цель на нанесении ущерба пользователям сети (абонентам), в свою очередь, делится на активы и пассивные.

Целью *активных угроз* является нарушение процесса его нормативного регулирования путем целенаправленного воздействия на аппаратные, программные и информационные ресурсы сети. Активным угрозам присуще следующее:

- нарушение работы линий связи сети передачи данных или радиоэлектронное подавление;
- нарушение работы компьютера (сервера) или его операционной системы;
- модификация данных действующей базы данных или нарушение сетевой информации;
- нарушение или модификация операционной системы сети и др.

Источником таких нарушений могут быть непосредственные действия злоумышленника, программные вирусы и т.п.

*Пассивные угрозы,* как правило, предназначены для несанкционированного использования информационных ресурсов без ущерба для производительности сети. В качестве примера можно привести попытку получения циркулирующей в них информации прослушиванием каналов передачи данных.

В зависимости от местоположения источника угрозы могут быть *внешними* и *внутренними.*

*Внешним угрозам информационной безопасности* свойственны следующее:

- деятельность внешней разведки и специальных служб;
- деятельность конкурирующих экономических структур;
- деятельность отдельных лиц и преступных групп внутри страны, направленная против интересов и структур граждан, государства и общества в целом;
- стихийное бедствие и аварии.

*Внутренним угрозам информационной безопасности* свойственны следующее:

- нарушение требований, установленных в области безопасности информации, которое допускается сотрудниками и пользователями, предоставляющими услуги мобильным системам (по незнанию или умышленно);
- отказ и неисправность технических средств, средств эффективного контроля при обработке, хранении и передаче, средств защиты сообщений (данных); обновление программного обеспечения, и мер по обеспечению эффективного контроля работы программного обеспечения.

По способу осуществления угрозы можно разделить на следующие виды:

- организационные;
- программно-математические;
- радиоэлектроные;
- физические.

К *организационным видам угроз* можно отнести:

- нарушение требований, предъявляемых к информационной безопасности, которое допускается сотрудниками и пользователями мобильных систем;
- манипулирование информацией (дезинформация, расшифровка или изменение информации);
- несанкционированное копирование данных в мобильных системах;
- кража информации из базы данных мобильных систем и банка данных;
- кража машинного носителя информации;
- хищение важных криптографически защищенных документов;
- удаление или модификация данных в мобильных системах.

К *программно-математическим угрозам* информационной безопасности относятся:

- внедрение вирусных программ;
- использование программных закладок.

К *радиоэлектронным угрозам* информационной безопасности относятся:

- утечка информации в технических каналах связи;
- внедрение электронных технических средств защиты информации в помещениях;
- принудительно заставлять получать ложную информацию в сетях передачи данных и линиях связи;
- радиоэлектронное подавление линий связи и средств управления мобильных систем.

К *физическим угрозам* информационной безопасности относятся:

- нарушение средств сбора, обработки, передачи, защиты информации, целенаправленное внедрение неполадок;
- разрушение или поломка машинного носителя информации;
- негативное влияние на пользователей, обслуживающих мобильную систему с целью внедрения физических, программно-математических или организационных угроз.

## 5.2. Основные угрозы безопасности информации в мобильных системах

Использование беспроводной технологии дает большие преимущества. Если эта технология дает пользователям ощущение свободного перемещения без потери контакта, то для создателей сети она создаёт большие возможности по организации связи. Кроме того, эта технология способствует появлению многих новых устройств. Однако беспроводная технология несет в себе больше угроз по сравнению с обычными проводными сетями. Чтобы создать безопасное беспроводное приложение необходимо определить все направления беспроводной атак. К сожалению, приложения никогда не будут полностью безопасными, но тщательное изучение рисков, связанных с беспроводными технологиями, поможет повысить уровень их защиты. Итак, проанализировав все возможные угрозы, необходимо построить сеть так, чтобы можно было быть готовым к защите от нестандартных угроз и всевозможных "атак".

***Неконтролируемая территория***. Главное отличие между проводными и беспроводными сетями связано с абсолютно неконтролируемой областью между конечными точками сети. В достаточно широком пространстве сотовых сетей беспроводная среда никак не контролируется. Современные беспроводные технологии предлагают ограниченный набор средств управления всей областью развертывания сети. Это позволяет атакующим, находящимся в непосредственной близости от беспроводных структур, производить целый ряд нападений, которые были невозможны в проводном мире.

***Скрытное подслушивание.*** Наиболее распространенная проблема в таких открытых и неуправляемых средах, как беспроводные сети, - возможность анонимных атак. Анонимные вредители могут перехватывать радиосигнал и расшифровывать передаваемые данные, как показано на рис. 5.1. Чтобы перехватить передачу, злоумышленник должен находиться вблизи от передатчика. Перехваты такого типа практически невозможно зарегистрировать, и еще труднее им помешать. Использование антенн и усилителей дает злоумышленнику возможность находиться на значительном удалении от цели в процессе перехвата.

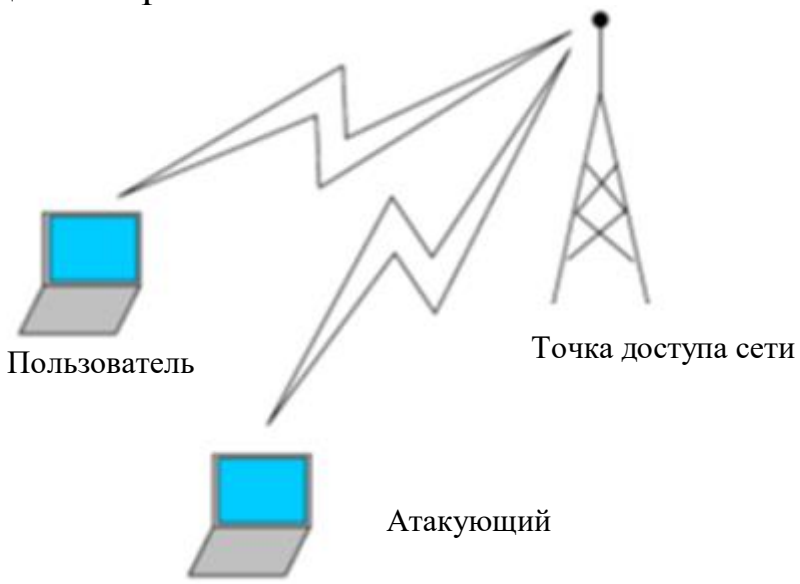



Рис. 5.1. Скрытное прослушивание в беспроводной сети

Другой способ подслушивания - подключиться к беспроводной сети. Активное подслушивание в локальной беспроводной сети (LAN) обычно основано на неправильном использовании протокола Address Resolution Protocol (ARP). Изначально эта технология была создана для "прослушивания" сети. В действительности мы имеем дело с атакой типа "man in the middle" (MITM - "человек в середине",

см. ниже) на уровне связи данных. Атакующий посылает ARP-ответы, на которые не было запроса, к целевой станции LAN, которая отправляет ему весь проходящий через нее трафик. Затем злоумышленник будет отсылать пакеты указанным адресатам. Таким образом, беспроводная станция может перехватывать трафик другого беспроводного клиента (или проводного клиента в локальной сети).

***Глушение.*** Глушение в сетях происходит тогда, когда преднамеренная или непреднамеренная интерференция превышает возможности отправителя или получателя в канале связи, таким образом, выводя этот канал из строя. Атакующий может использовать различные способы глушения.

*Отказ в обслуживании.* Полную парализацию сети может вызвать атака типа DoS (Denial of Service - отказ в обслуживании). Во всей сети, включая базовые станции и клиентские терминалы, возникает такая сильная интерференция, что станции не могут связываться друг с другом (рис. 5.2). Эта атака выключает все коммуникации в определенном районе. Атаку DoS на беспроводные сети трудно предотвратить или остановить. Большинство беспроводных сетевых технологий использует нелицензированные частоты - следовательно, допустима интерференция от целого ряда электронных устройств.

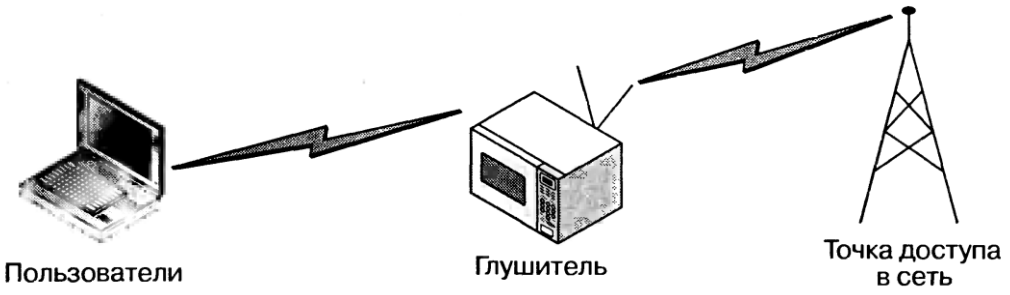



Рис. 5.2. Атаки глушения в беспроводных коммуникациях

*Глушение клиентов.* Глушение клиентской станции дает возможность мошеннику подставить себя на место заглушённого клиента, как показано на рис. 5.3. Также глушение могут использовать для отказа в обслуживании клиента, чтобы ему не удавалось реализовать соединение. Более изощренные атаки прерывают соединение с базовой станцией, чтобы затем она была присоединена к станции злоумышленника.


Рис. 5.3. Атака глушения клиента для перехвата соединения

*Глушение базовой станции.* Глушение базовой станции предоставляет возможность подменить ее атакующей станцией, как показано на рис. 5.4. Такое глушение лишает пользователей доступа к услугам, а телекоммуникационные компании - их прибылей.


Рис. 5.4. Атака глушения базовой станции
для перехвата соединения

Как отмечалось выше, большинство беспроводных сетевых технологий использует нелицензированные частоты. Поэтому многие устройства - радиотелефоны, системы слежения и микроволновые печи - могут влиять на работу беспроводных сетей и глушить беспроводное соединение. Чтобы предотвратить такие случаи непреднамеренного глушения, прежде чем покупать дорогостоящее беспроводное оборудование, надо тщательно проанализировать место его установки. Такой анализ поможет убедиться в том, что другие устройства никак не помешают коммуникациям, а также удержит вас от бессмысленных трат.

***Вторжение и модификация данных.*** Вторжение происходит, когда злоумышленник добавляет информацию к существующему потоку данных, чтобы перехватить соединение или пересылать данные либо команды в своих целях. Атакующий может манипулировать управляющими командами и потоками информации, отсылая пакеты или команды на базовую станцию, и наоборот.

Подавая управляющие команды в нужный канал управления, можно добиться отсоединения пользователей от сети Вторжение может использоваться для отказа в обслуживании. Атакующий переполняет точку доступа в сеть командами соединения, "обманув" ее превышением максимума возможных обращений, - таким образом, другим пользователям будет отказано в доступе.

***Атака "man in the middle".*** Атаки типа MITM (man in the middle - "человек в середине") аналогичны вышеописанным вторжениям. Они могут принимать различные формы и используются для разрушения конфиденциальности и целостности сеанса связи. Атаки MITM более сложны, чем большинство других атак: для их проведения требуется подробная информация о сети. Злоумышленник обычно подменяет идентификацию одного из сетевых ресурсов. Когда жертва атаки инициирует соединение, мошенник перехватывает его и затем завершает соединение с требуемым ресурсом, а потом пропускает все соединения с этим ресурсом через свою станцию, как показано на рис. 5.5. При этом атакующий может посылать информацию, изменять посланную или подслушивать все переговоры и потом расшифровывать их.

***Абонент-мошенник.*** После тщательного изучения работы абонента сети атакующий может "притвориться" им или клонировать его клиентский профиль, чтобы попытаться получить доступ к сети и ее услугам. Кроме того, достаточно украсть устройство для доступа, чтобы войти в сеть. Обеспечение безопасности всех беспроводных устройств - дело очень непростое, поскольку они намеренно делаются небольшими для удобства передвижения пользователя.

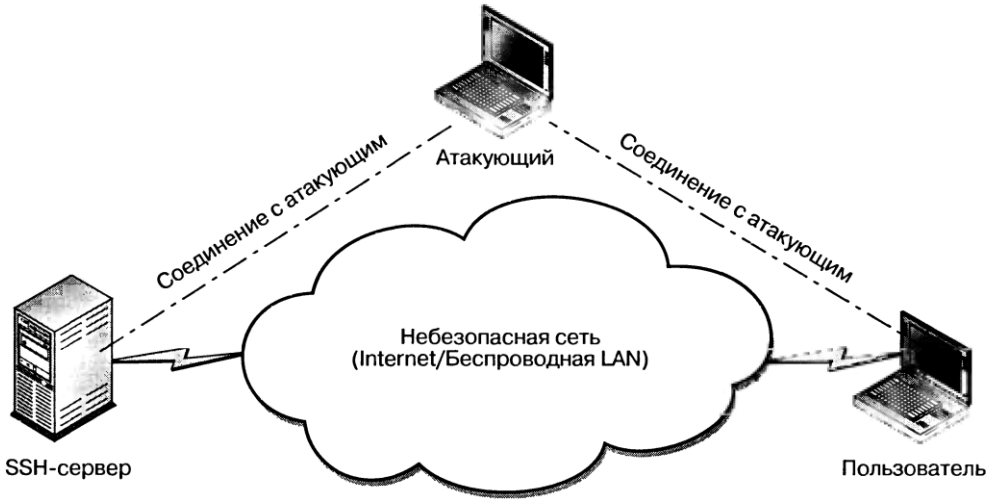



Рис. 5.5. Атака типа MITM

***Ложные точки доступа в сеть.*** Опытный атакующий может организовать ложную точку доступа с имитацией сетевых ресурсов. Абоненты, ничего не подозревая, обращаются к этой ложной точке доступа и сообщают ей свои важные реквизиты, например аутентификационную информацию. Этот тип атак иногда применяют в сочетании с прямым глушением, чтобы «заглушить» истинную точку доступа в сеть (рис. 5.6).

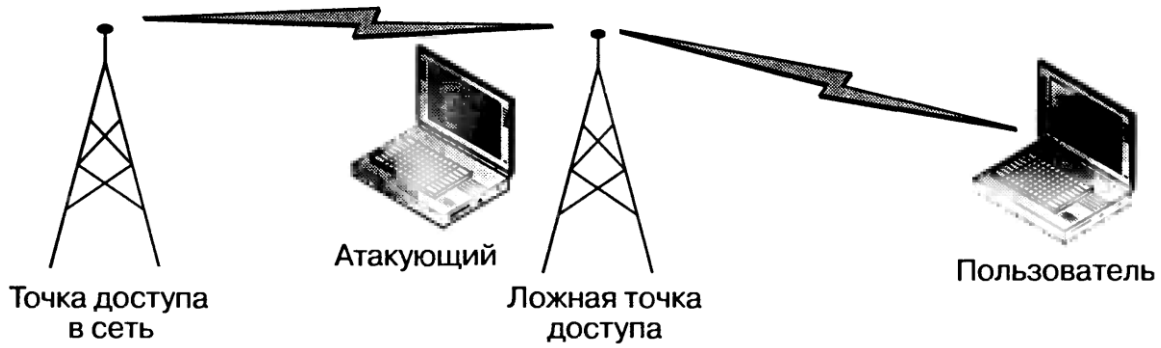



Рис. 5.6. Ложная точка доступа

Пользователи, имеющие доступ к проводной сети, могут также способствовать установлению ложных точек доступа, ненамеренно открывая сеть для нападений. Иногда пользователь устанавливает беспроводную точку доступа, стремясь к удобствам, которые предоставляет беспроводная связь, но не задумываясь о проблемах безопасности. Сегодня оборудование для точек доступа можно купить в любом магазине электроники за умеренную цену. Эти точки могут оказаться "черным ходом" для проникновения в проводную сеть, поскольку обычно они устанавливаются в такой конфигурации, которая подвержена всевозможным атакам.

***Анонимность атак.*** Беспроводной доступ обеспечивает полную анонимность атаки. Без соответствующего оборудования в сети, позволяющего определять местоположение, атакующий может легко сохранять анонимность и прятаться где угодно на территории действия беспроводной сети. В таком случае злоумышленника трудно поймать и еще сложнее передать дело в суд.

Важно отметить, что многие мошенники изучают сети не для атак на их внутренние ресурсы, а для получения бесплатного анонимного доступа в Internet, прикрываясь которым они атакуют другие сети.

***Атаки типа "клиент-клиент".*** Практически все абоненты сети могут быть атакованы. После первого успеха атакующий получает право на доступ к корпоративной или телекоммуникационной сети. Большинство сетевых администраторов не уделяет должного внимания ужесточению режима безопасности или установке персональных межсетевых экранов (firewalls). Поэтому успешные атаки на клиентов беспроводной сети могут открыть злоумышленникам имена пользователей и их пароли, а следовательно, и доступ к другим сетевым ресурсам.

***Атаки на сетевое оборудование.*** Неправильно сконфигурированное оборудование - первая приманка для атакующих: обычно оно открывает путь для дальнейшего проникновения в сеть (иногда здесь используют метафору «камешки для перехода через реку»). Этот путь могут избрать для того, чтобы обойти контроль доступа. Главные объекты атак на оборудование - такие сетевые устройства, как маршрутизаторы, переключатели, серверы для хранения архивов и серверы доступа.

***Тайные беспроводные каналы.*** Есть еще один фактор, который пользователи беспроводных систем должны принимать во внимание, создавая или оценивая сеть. Поскольку стоимость точек беспроводного доступа низка и создать точку доступа на основе ПО, стандартного ноутбука и NIC-карты для беспроводной связи довольно просто, требуется бдительно отслеживать некорректно сконфигурированное или непродуманно развернутое беспроводное оборудование в проводной сети (рис. 5.8, где показан так называемый черный ход в сеть). Это оборудование может проделать очень заметные "дыры" в проводной инфраструктуре, куда могут направиться атакующие с расстояния в несколько километров от сети.

***Проблемы роуминга.*** Еще одно важное отличие проводных и беспроводных технологий заключается в способности пользователя передвигаться, поддерживая связь с сетью. Концепция роуминга практически одинакова в различных стандартах беспроводной связи - CDMA (Code Division Multiple Access), GSM (Global System for Mobile Communications) и беспроводном Ethernet. Многие сетевые приложения TCP/IP требуют, чтобы IP-адреса сервера и клиента оставались неизменными, однако в процессе роуминга в сети абонент обязательно будет покидать одни ее участки и присоединяться к

другим. На этом требовании основано использование мобильных IP-адресов и других механизмов роуминга в беспроводных сетях.

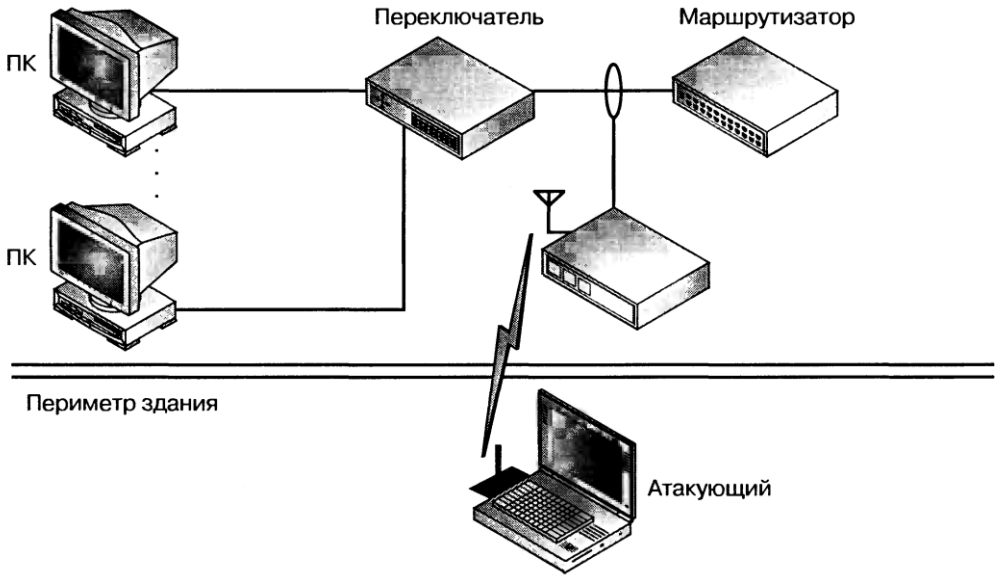



Рис. 5.8. Точка доступа в виде "черного хода" в сеть

Главная идея мобильной IP-связи - регистрация местонахождения пользователя и перенаправление трафика. Адрес, не зависимый от того, где находится абонент, предназначен для поддержки TCP/IP-соединения, а временный адрес, зависящий от местонахождения пользователя, обеспечивает соединение с ресурсами локальной сети. Для мобильной системы IP есть три дополнительных регулирующих требования: мобильный узел (МУ), домашний агент и иностранный агент. МУ - это беспроводное устройство пользователя, ДА - сервер, расположенный в домашней сети МУ, а ИА - сервер, расположенный в сети, куда пойдет роуминг. Когда МУ переходит в новую сеть, он получает временный IP-адрес, зависящий от местоположения, и регистрируется в ИА. Затем ИА связывается с ДА, уведомляя его, что МУ присоединен к нему и все пакеты должны с этого момента перенаправляться через ИА-роуминг на ДА.

***Угрозы криптозащиты.*** В сотовых сетях CDMA, GSM и беспроводной Ethernet-сети применяются криптографические средства для обеспечения целостности и конфиденциальности информации. Однако оплошности приводят к нарушению коммуникаций и злонамеренному использованию информации.

WEP (Wired Equivalent Privacy - секретность на уровне проводной связи) - это криптографический механизм, созданный для обеспечения безопасности сетей типа 802.11. Ошибки при внедрении WEP и проблемы управления сделали его практически бесполезным. Этот механизм разработан с единственным статическим ключом, который применяется всеми пользователями. Управляющий доступ к ключам, частое их изменение и обнаружение нарушений практически невозможны. Исследование внедрения алгоритма RC4 в WEP выявило уязвимые места, из-за которых атакующий может полностью восстановить ключ после захвата минимального сетевого трафика. В Internet есть средства, которые позволяют злоумышленнику восстановить ключ в течение нескольких часов. Поэтому на WEP нельзя полагаться как на средство аутентификации и конфиденциальности в беспроводной сети.

## 5.3. Модель нарушителя безопасности информации

Для предотвращения возможных угроз фирмы должны не только обеспечить защиту операционных систем, программного обеспечения и контроль доступа, но и попытаться выявить категории нарушителей и те методы, которые они используют.

В зависимости от мотивов, целей и методов, действия нарушителей безопасности информации можно разделить на четыре категории:

– искатели приключений;

– идейные хакеры;

– хакеры-профессионалы;

– ненадежные (неблагополучные) сотрудники.

*Искатель приключений,* как правило, молод: очень часто это студент или старшеклассник, и у него редко имеется продуманный план атаки. Он выбирает цель случайным образом и обычно отступает, столкнувшись с трудностями. Найдя дыру в системе безопасности, он старается собрать закрытую информацию, но практически никогда не пытается ее тайно изменить. Своими победами такой искатель приключений делится только со своими близкими друзьями-коллегами.

*Идейный хакер* - это тот же искатель приключений, но более искусный. Он уже выбирает себе конкретные цели на основании своих убеждений. Его излюбленным видом атаки является изменение

информационного наполнения Web-сервера или, в более редких случаях, блокирование работы атакуемого ресурса. По сравнению с искателем приключений, идейный хакер рассказывает об успешных атаках гораздо более широкой аудитории.

*Хакер-профессионал* имеет четкий план действий и нацеливается на определенные ресурсы. Его атаки хорошо продуманы и обычно осуществляются в несколько этапов. Сначала он собирает предварительную информацию (тип ОС, предоставляемые сервисы и применяемые меры защиты). Затем он составляет план атаки с учетом собранных данных и подбирает (или даже разрабатывает) соответствующие инструменты. Далее, проведя атаку, он получает закрытую информацию, и, наконец, уничтожает все следы своих действий. Такой атакующий профессионал обычно хорошо финансируется и может работать в одиночку или в составе команды профессионалов.

*Ненадежный сотрудник* своими действиями может доставить столько же проблем (или даже больше), сколько промышленный шпион, к тому же его присутствие обычно сложнее обнаружить. Кроме того, ему приходится преодолевать не внешнюю защиту сети, а только, как правило, менее жесткую внутреннюю. Он не так изощрен в способах атаки, как промышленный шпион, и поэтому чаще допускает ошибки и тем самым может выдать свое присутствие. Однако в этом случае опасность его несанкционированного доступа к корпоративным данным много выше, чем любого другого злоумышленника.

Перечисленные категории нарушителей безопасности информации можно сгруппировать по их квалификации: начинающий (искатель приключений), специалист (идейный хакер, ненадежный сотрудник), профессионал (хакер-профессионал). А если с этими группами сопоставить мотивы нарушения безопасности и техническую ос-нащенность каждой группы, то можно получить обобщенную модель нарушителя бе-зопасности информации, как это показано на рис. 5.10.

Нарушитель безопасности информации, как правило, являясь специалистом определенной квалификации, пытается узнать все о компьютерных системах и сетях и, в частности, о средствах их защиты. Поэтому модель нарушителя определяет:

– категории лиц, в числе которых может оказаться нарушитель;

– возможные цели нарушителя и их градации по степени важности и опасности;

– предположения о его квалификации;

– оценка его технической вооруженности;

– ограничения и предположения о характере его действий.

До недавнего времени вызывали беспокойство случаи, когда недовольные руководителем служащие, злоупотребляя своим положением, портили системы, допуская к ним посторонних или оставляя системы без присмотра в рабочем состоянии. Побудительными мотивами таких действий являются:

– реакция на выговор или замечание со стороны руководителя;

– недовольство тем, что фирма не оплатила сверхурочные часы работы;

– злой умысел в качестве, например, реванша с целью ослабить фирму как конкурента какой-либо вновь создаваемой фирмы.


Рис. 5.10. Модель нарушителя безопасности информации

Недовольный руководителем служащий создает одну из самых больших угроз вы-числительным системам коллективного пользования. Это обусловлено еще и тем, что агентства по борьбе с

хакерами с большей охотой обслуживают владельцев индивидуальных компьютеров.

Профессиональные хакеры - это компьютерные фанаты, прекрасно знающие вычислительную технику и системы связи. Они затратили массу времени на обдумывание способов проникновения в системы и еще больше, экспериментируя с самими системами. Для вхождения в систему профессионалы чаще всего используют некоторую систематику и эксперименты, а не рассчитывают на удачу или догадку. Их цель - выявить и преодолеть защиту, изучить возможности вычислительной установки и затем удалиться, утвердившись в возможности достижения своей цели. Благодаря высокой квалификации эти люди понимают, что степень риска мала, так как отсутствуют мотивы разрушения или хищения.

К категории хакеров-профессионалов обычно относят следующих лиц:

– входящих в преступные группировки, преследующие политические цели;

– стремящихся получить информацию в целях промышленного шпионажа;

– хакер или группировки хакеров, стремящихся к наживе.

Компьютерные махинации обычно тщательно спланированы и совершаются со знанием дела. Мотивом нарушений, как правило, служат большие деньги, которые можно было получить, практически не рискуя. Вообще профессиональные пираты стремятся свести риск к минимуму. Для этого они привлекают к соучастию работающих или недавно уволившихся с фирмы служащих, поскольку для постороннего риск быть обнаруженным при проникновении в банковские системы весьма велик.

Сегодня, когда Интернет уже стучится в дверь каждого дома, хакеры становятся настоящим бедствием для государственных и корпоративных компьютерных сетей.

# ГЛАВА 6. БЕЗОПАСНОСТЬ МОБИЛЬНЫХ ОПЕРАЦИОННЫХ СИСТЕМ

## 6.1. Мобильные операционные системы

Существующие на данный момент мобильные операционные системы (ОС) предоставляют пользователям возможности не только по осуществлению привычных для мобильных телефонов действий, таких как отправка SMS-сообщений и совершение телефонных вызовов, но и широкие возможности по хранению, редактированию и обмену данными.

При этом некоторые из существующих на данный момент мобильных ОС предоставляют пользователям дополнительные возможности по зашифрованному хранению данных, а также по удаленному управлению данными на мобильном устройстве в случае его утери или кражи.

Анализ наличия данных возможностей может быть проведен только в случае, если исходные коды ОС полностью открыты.

Таким образом, для создания классификации мобильных ОС были выбраны следующие параметры (рис. 6.1):

- открытость операционной системы;
- наличие средств защиты информации (СЗИ);
- наличие средств криптографической защиты информации (СКЗИ);
- типы конечных устройств – планшеты, мобильные телефоны.

Далее рассмотрены самые распространенные операционные системы для мобильных устройств: Symbian OS, Windows Mobile, Linux-системы (Android), Palm OS, iPhone OS, BlackBerry OS.

***Symbian OS***

Была самой популярной ОС для мобильных устройств благодаря поддержке фирмы Nokia. Важную роль также сыграло то, что система имеет небольшой размер, а также то, что графический интерфейс и ядро системы отделены друг от друга. Это позволило легко устанавливать ее для различных мобильных устройств. Позднее была добавлена многозадачность.

Каждый разработчик создавал свой дистрибутив (версию) этой операционной системы в зависимости от ограничений аппаратной платформы, под которую она разрабатывалась. Каждая версия обладала своими особенностями, что делало необходимым под

каждую версию разрабатывать свои приложения. Это было неудобно, поэтому после появления Windows Mobile, Android и iPhoneOS утратила свою популярность среди производителей мобильных девайсов.


Рис. 6.1. Классификация мобильных операционных систем

На данный момент из крупных производителей мобильных девайсов только компания Nokia использует эту ОС для своих смартфонов.

*Достоинства:*

- низкие требования к памяти и процессору;
- функция освобождения неиспользуемой памяти;
- стабильность;
- малое количество вирусов для этой платформы;
- быстро выходят новые версии и исправляются нестабильности;
- большое количество программ.

*Недостатки:*

- для связи с ПК нужно устанавливать дополнительный софт;
- несовместимость программ для старых и новых версий.

***Windows Mobile***

Эта операционная система разработана мировым лидером в производстве операционных систем – компанией Microsoft. Эта система использует такой же программный интерфейс, что и в

персональных компьютерах. Это делает написание программ более простым, а пользователям нравится удобный и понятный интерфейс, знакомый им с настольной Windows. Windows Mobile является компонентной, многозадачной, многопоточной и многоплатформенной операционной системой. Благодаря этому она сыскала широкое распространение на мобильных устройствах.

*Достоинства:*

- схожесть с настольной версией;
- удобная синхронизация;
- в комплекте идут офисные программы;
- многозадачность.

*Недостатки:*

- высокие требования к оборудованию;
- наличие большого числа вирусов;
- нестабильности в работе.

***Android***

Android - одна из самых молодых мобильных ОС, основанная на базе операционной системы Linux и разрабатываемая Open Handset Alliance (OHA) при поддержке Google. Исходный код находится в открытом доступе, благодаря чему любой разработчик может создать свою версию этой мобильной ОС. Разработчикам приложений выдвинуто небольшое количество ограничений, благодаря чему существует множество как платных, так и бесплатных приложений, которые можно удобно загрузить с Android Market.

*Достоинства:*

- гибкость;
- открытые исходные коды;
- множество программ;
- высокое быстродействие;
- удобное взаимодействие с сервисами от Google;
- многозадачность.

*Недостатки:*

- множество актуальных версий – для многих устройств новая версия входит слишком поздно или не появляется вовсе, поэтому разработчикам приходится разрабатывать приложения, ориентируясь на более старые версии;
- высокая предрасположенность к хакерским атакам из-за открытости кода;
- почти всегда требует доработок.

***iOS***

Мобильная операционная система от компании Apple. Данная система получила распространение только на продуктах компании Apple. Применяется в смартфонах iPhone, плеерах iPod, планшетах iPad а также телевизионной приставке Apple TV.

*Достоинства:*

- удобство пользования;
- качественная служба поддержки;
- регулярные обновления, устраняющие многие проблемы в работе;
- возможность купить в App Store множество различных программ.

*Недостатки:*

- необходимость джайлбрейка для установки неофициальных приложений;
- заблокированный характер ОС;
- отсутствие многозадачности;
- нет встроенного редактора документов.

***Palm OS***

Данная операционная система появилась в 1996 году. Применялась в КПК. Была очень распространена из-за широких возможностей и удобства пользователей. К настоящему моменту практически не применялась, но в этом году разработчика поглотила компания HP. Благодаря этому появились надежды на воскрешение некогда популярной среди КПК операционной системы.

*Достоинства:*

- нетребовательна к ресурсам;
- очень удобный интерфейс пользователя;
- удобная синхронизация с ПК;
- надежность.

Недостатки:

- отсутствует полноценная многозадачность;
- не развиты мультимедийные функции.

***BlackBerry OS***

Операционная система работает исключительно на устройствах, выпускаемых компанией *Research In Motion Limited* (RIM). Ориентирована на корпоративных пользователей. Свое название получила от смартфонов для которых создавалась, так как клавиатура смартфонов были похожи на ягоду ежевики. Смартфоны с этой

операционной системой получили распространение в корпоративной среде, благодаря сложности перехвата сообщений.

*Достоинства:*

- удобное пользование электронной почтой;
- легкая синхронизация с ПК;
- широкие возможности настроек безопасности.

*Недостатки:*

- оптимизирована для вывода только текстовой информации, качество работы с графикой не очень хорошее;
- не очень удобный браузер.

Как видим, технические характеристики устройства - отнюдь не главный параметр при выборе мобильного девайса. Ведь смысла от аппарата, который напичкан самым современным железом, но который работает на операционной системе с небольшими возможностями, минимален.

## 6.2. Безопасность мобильных операционных систем и механизмы ее реализации

Развитие механизмов безопасности для мобильных устройств шло по другому пути, нежели для персональных компьютеров. Механизмы безопасности должны были обеспечивать более жесткие требования к защищенности мобильного устройства.

Эти жесткие требования к защищенности должны обеспечить:

- идентификацию устройства (International Mobile Equipment Identifier, IMEI), т.е. устройство должно быть защищено от "манипуляций и изменений любыми средствами, включая механические, электрические и программные";
- защищенное хранение радиочастотных настроек, откалиброванные на этапе производства мобильного устройства;
- надежность операционной системы, не допускающей появления критической ошибки системы, присущей в операционной системе Windows, так называемый "синий экран смерти", после которой ОС уходит в перезагрузку, теряя все несохраненные данные;
- доступность системного раздела только для чтения и разграничение выполняемых процессов на уровне ядра.

Основные различия в механизмах безопасности операционных систем Android и iOS следующие:

- различные принципы разграничения доступа на уровне ядра операционной системы;
- различные модели процесса верификации загружаемого в магазины программного обеспечения;
- различные принципы контроля прав доступа устанавливаемых приложений.

Чтобы обеспечить выполнение этих требований были созданы и внедрены защитные механизмы программного и аппаратного уровня.

Расмотрим более подробно защитные механизмы программного и аппаратного уровня на примере широко распространенного процессора ARM TrustZone. Этот процессор имеет архитектуру Advanced RISC Machine (ARM) с сокращенным набором команд (RISC), который устанавливается в большинстве смартфонов и планшетов.

Защитные механизмы программного уровня в процессорах типа TrustZone.

В основе концепции ARM TrustZone лежит разделение на уровне аппаратуры среды выполнения на защищенную (trusted), или иначе *безопасная среда исполнения TEE*) и незащищенную (non-trusted), или иначе *доступная среда исполнения REE* (рис. 6.2).

Этот подход затрагивает не только процессор, но и память, транзакции на шинах, прерывания, периферийные устройства в рамках "системы-на-чипе" System-on-a-Chip (SoC), которые используют несколько многоядерных процессоров, предназначенных для встраиваемых приложений. SoC - это электронная схема, выполняющая функции целого устройства (например, компьютера) и размещенная на одной интегральной схеме.

Для удобства объяснений введем терминологию:

*Rich OS* - полнофункциональная операционная система, работающая в доступной среде REE – это набор библиотек, сервисов и услуг, которые обеспечивают общие функции управления компонентами системы - внутренних и сторонних приложений.

*Secure OS* - доверенная операционная система, работающая в безопасной среде исполнения TEE и ограниченная в функциях ради безопасности. Среда TEE реализуется с использованием защищенного режима работы процессора.

*Trustlet* – проверенное приложение, запущенное в Secure OS, которое может быть предоставлено сторонними разработчиками.

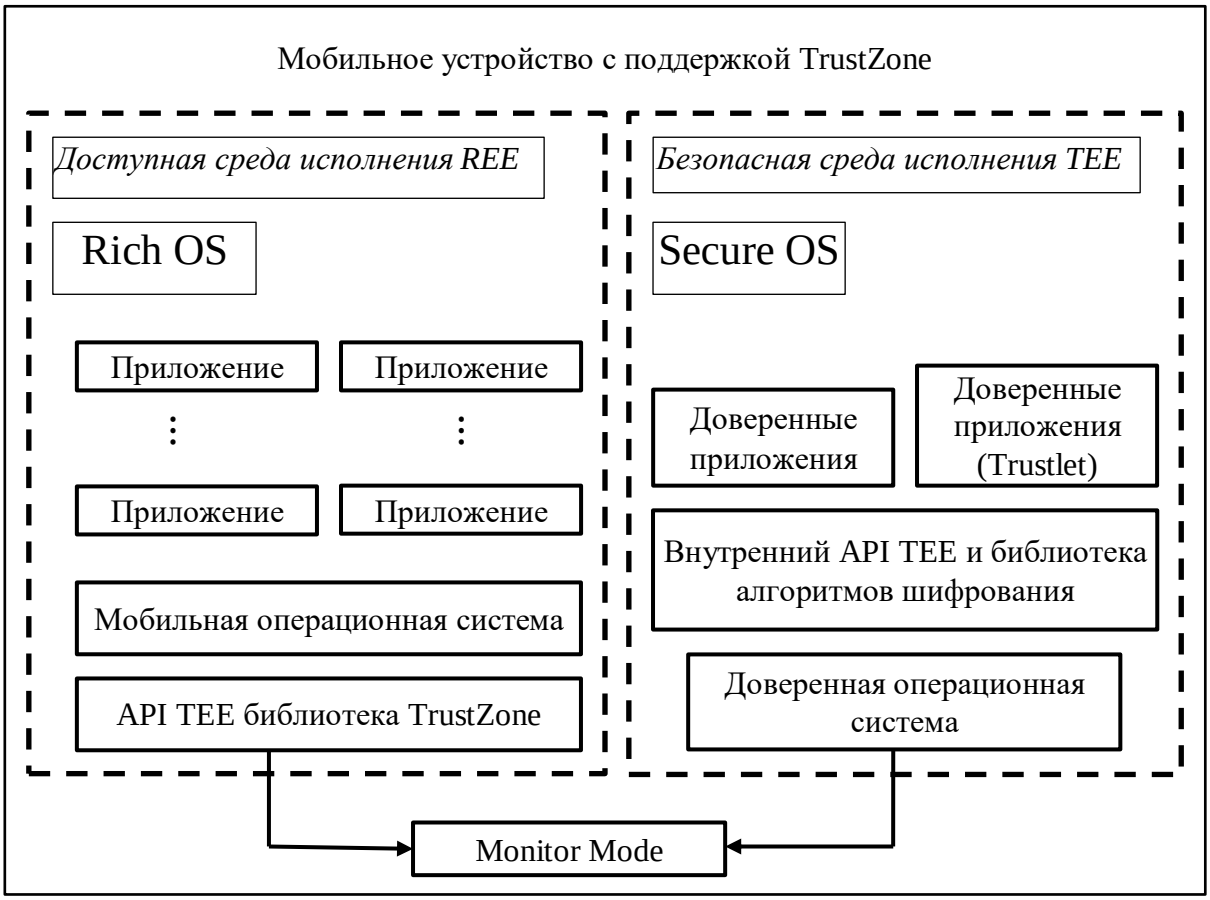



Рис. 6.2. Архитектура программного обеспечения мобильных устройств с поддержкой TrustZone

*TEE* - это Trusted Execution Environments, совокупность аппаратных (TrustZone) и программных (Secure OS + приложения) средств обеспечения безопасности критически важных компонентов.

*REE* – это Rich Execution Environment, мобильная операционная система, которая работает с приложениями мобильного устройства.

Среда TEE обеспечивает целостность платформы при загрузке, защищенное хранение данных, идентификацию устройств, изолированное выполнение программного кода и функции аутентификации устройства.

Так что же представляют собой эти среды исполнения - TEE и REE? По большому счету, разницы особой нет. В обоих есть все возможные режимы процессоров (supervisor, user, data abort и т.д.) исключая Monitor Mode, который всегда защищен.

*Monitor mode* представляет собой мощный инструмент для мониторинга мобильной системы. С его помощью можно:

- контролировать процессы, т.е. просматривать все запущенные процессы с возможностью быстрой остановки ненужных;

- осуществлять мониторинг сетевых интерфейсов, т.е. просматривать все используемые на данный момент сетевые интерфейсы.

- просматривать и осуществлять мониторинг сетевой активности, т.е. предоставлять детальную информацию о каждом подключении, информацию о сетевом IP-адресе, используемом при подключении;

- осуществлять сбор информации об используемой памяти, заряде аккумулятора, состояния файловой системы;

- просматривать все системные сообщения в реальном времени.

Процедура загрузки и разделения сред (TEE или REE) обычно выглядит так.

Процессор стартует в режиме Monitor Mode, то есть, находится в безопасной среде исполнения TEE, и инициирует загрузку Bootloader (Загрузчик BL - bootloader – программа, которая контролирует ядро операционной системы, чтобы процесс загрузки шел в нормальном режиме) в, так называемой, Secure OS, которая будет основой нашего TEE. TEE настраивает всю необходимую безопасную конфигурацию системы. Например, она закрывает сканер отпечатков пальцев и часть оперативной памяти от доступа из доступной среды REE. После этого инициируется переход в TEE, где уже другой загрузчик, например GRUB (GRand Unified Bootloader) - загрузчик операционной системы, позволяет пользователю иметь несколько установленных операционных систем и при включении компьютера выбирать одну из них для загрузки. Далее запускается Rich OS в обычном порядке. Упрощенный алгоритм этого процесса иллюстрирует рис. 6.3.

Таким образом, ARM TrustZone обеспечивает защищённое хранение данных в зашифрованном виде, генерацию ключей на основе базового ключа и обеспечивает проверку подписей. Классические примеры использования - это защита электронных платежей, проприетарного т.е. частного, патентованного программного обеспечения (proprietary software), видео/аудио контента, аутентификация всевозможных данных.

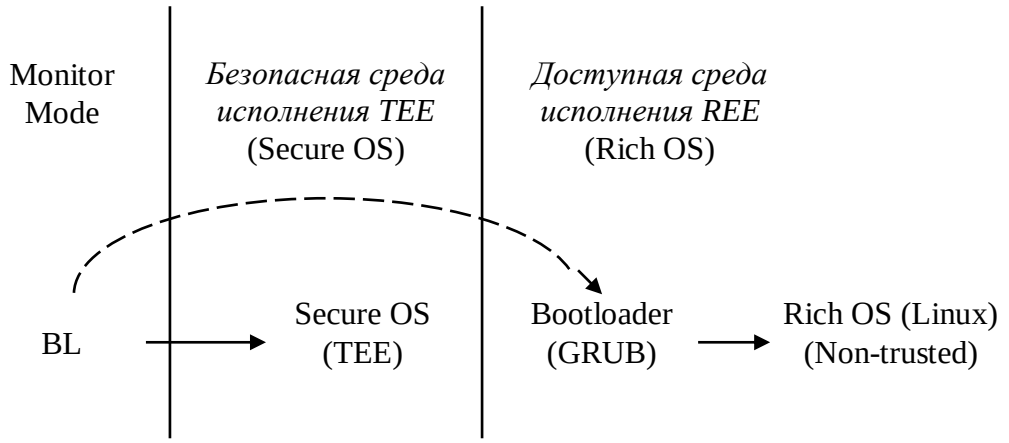



Рис. 6.3. Упрощенный алгоритм процедуры загрузки
и разделения сред на REE и TEE

*Защитные механизмы аппаратного уровня в процессорах типа TrustZone* реализованы следующим образом. В мобильных устройствах механизм аппаратной защиты информации состоит из центрального процессора, имеющего небольшое количество постоянной и оперативной памяти, контроллеров периферийных устройств и прерываний, а также портов отладки и трассировки, которые интегрированы в едином, главном чипе. Элементы, встроенные в такой процессор, соединены общей шиной. Остальные компоненты мобильного устройства: основная оперативная память, флэш-память, дисплей, антенна и т. д., реализованы отдельно от главного чипа (рис. 6.4).

Управление доступом к аппаратным элементам реализовано с помощью *флага состояния*, определяющего режим работы процессора: защищенный или штатный. Флаг состояния передается по коммуникационной шине центрального процессора.

Центральный процессор может работать в обычном или защищенном режимах, предназначенных соответственно для REE и TEE. В защищенном режиме (TEE) происходят загрузка и настройка, а затем включается нормальный режим (REE). При выполнении определенных команд возможны переключения в защищенный режим.

Доверенные приложения (Trustlet) выполняются, как уже сказано, в TEE, изолированной от REE.

Мобильная операционная система из REE обращается к сервисам TEE с помощью библиотеки TrustZone через Monitor Mode. В TEE доверенные приложения выполняются в среде доверенной

операционной системы с минимальной функциональностью, т.е. центральным процессором механизма аппаратной защиты информации. Эта операционная система предоставляет собой внутренний интерфейс программирования TEE, которым доверенные приложения могут пользоваться для связи с приложениями REE, а также для вызова функций криптографии и защищенного хранения.

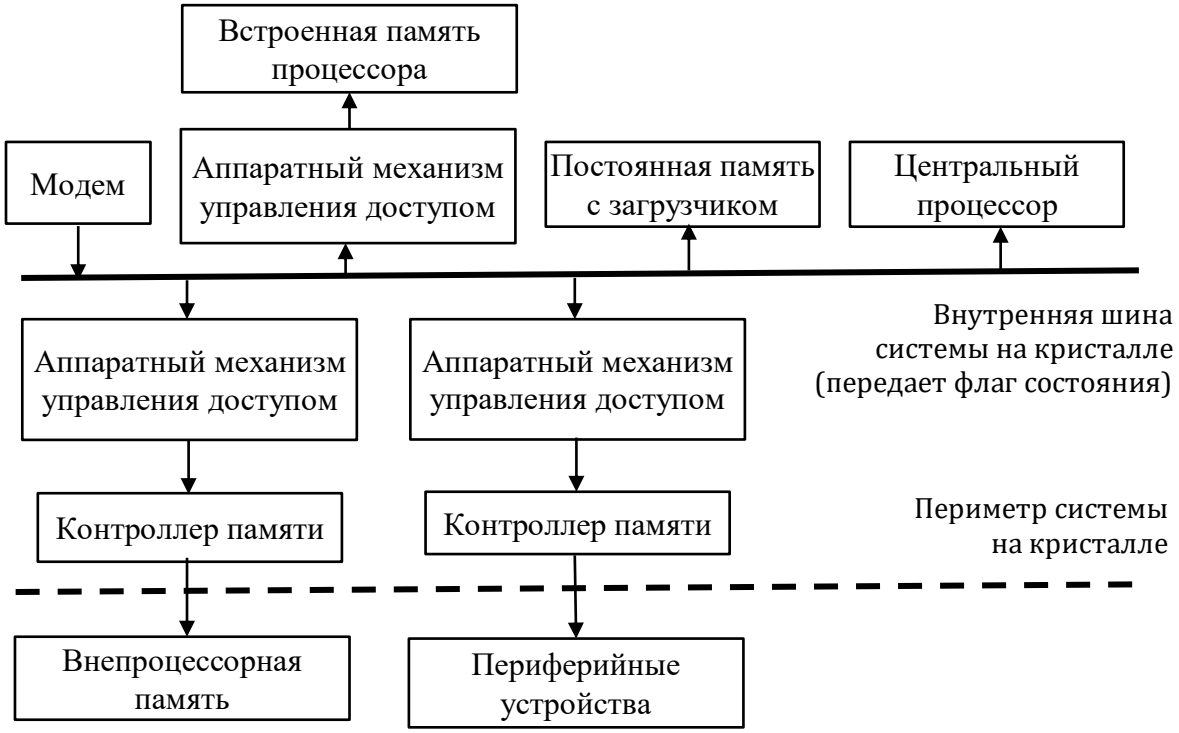



Рис. 6.4. Пример аппаратной конфигурации мобильного устройства с TrustZone

Подходы к обеспечению безопасности становятся комплексными и охватывают большую часть системы - как программные, так и аппаратные модули. Комплексный подход обеспечивает недостижимую ранее гибкость программного подхода с надежной защитой со стороны аппаратной части. Это дает возможность не ограничиваться заранее установленным на устройство набором функций, а программно и безопасно обновлять систему со временем.

## 6.3. Сравнительный анализ механизмов обеспечения безопасности в Android и iOS

Всех заинтересованных в защищенности мобильных смартфонов можно условно разбить на три категории: компании-разработчики, рядовые пользователи, либо владельцы продукта и корпорации. Рассмотрим основные механизмы защиты операционных систем Android и iOS и их эффективность с точки зрения каждой из сторон.

1. С точки зрения компаний-разработчиков основной риск безопасности - взлом их приложения и, как следствие, потеря клиентов и бизнеса. Если рассматривать способность мобильных приложений противостоять локальным и веб-атакам, то обе операционные системы как Android, так и iOS находятся примерно в равных условиях.

2. Приложения для Android представляют собой программы, написанные на языке Java, который невосприимчив к атакам на переполнение буфера, в отличие от программ для iOS, написанных на языке Objective-C. Приложения, написанные на Objective-C, потенциально уязвимы к переполнению буфера, однако в арсенале iOS-разработчиков присутствуют необходимые механизмы, способные предотвратить такие уязвимости. К таким механизмам, прежде всего, относятся параметры компиляции, такие как PIE (Position Independent Executable), SSP (Stack Smashing Protection) и ARC (Automatic Reference Counting). Данные параметры обеспечивают эффективное управление памятью и отсутствие ошибок, которые приводят к переполнениям буфера. В дополнение к этому на презентации восьмой версии iOS был представлен новый язык программирования Swift, призванный заменить собой Objective-C. По заявлениям компании Apple, новый язык является более простым в изучении и более безопасным, чем его предшественник.

Таким образом, Android- и iOS-приложения могут быть одинаково хорошо защищенными, и вероятность взлома этих приложений напрямую зависит от мастерства разработчиков.

3. Безопасность рядовых пользователей мобильных устройств зависит от безопасности мобильной ОС, которой они пользуются. Даже если на смартфоне установлены только хорошо защищенные приложения, конечные пользователи все равно могут быть успешно атакованы через бреши в самой операционной системе. Если по

критерию защищенности мобильных приложений обе ОС находятся на примерно одинаковом уровне, то *с точки зрения безопасности самой системы Android и iOS значительно различаются между собой.*

4. В механизмах защиты двух ОС, стоит отметить наличие в них базовых принципов безопасности, таких как *доступность системного раздела только для чтения и разграничение выполняемых процессов на уровне ядра.* И в Android, и в iOS системный раздел не доступен для записи, что предотвращает случайное либо целенаправленное изменение файлов системы. Также в обоих ОС реализован принцип "песочницы" (sandbox). Это значит, что каждое приложение работает в изолированном контейнере и не имеет доступа к системным файлам либо ресурсам других приложений.

5. Основные различия в механизмах безопасности Android и iOS относятся к принципам разграничения доступа на уровне ядра, к процессу верификации загружаемого в магазины ПО и к принципам контроля прав доступа устанавливаемых приложений.

6. Меры, предпринимаемые разработчиками по обеспечению отсутствия вредоносного программного обеспечения:

- в магазине приложений App Store. iOS-приложения тщательно проверяются на наличие уязвимостей и на соответствие стандартам разработки Apple. Каждое приложение, устанавливаемое на iOS, подписывается уникальным сертификатом программы "iOS Developer Program", который выдается компанией Apple только после необходимых верификаций разработчика. В iOS раздача прав доступа приложениям реализована гибко. Каждая категория доступа, будь то доступ к камере или к GPS, должна быть подтверждена либо отклонена пользователем;

- в Google Play перед загрузкой приложения не проверяются, но проводится регулярные сканирования своего магазина на предмет наличия потенциально вредоносного ПО. При установке нового приложения на устройство под управлением Android пользователю показывается полный перечень прав доступа, требуемых данному приложению. По этому перечню пользователь может определить потенциально вредоносное ПО и отменить его установку.

7. Уязвимости самих операционных систем:

- iOS, несмотря на то, что она полностью открытая ОС, она опережает Android по количеству известных уязвимостей (CVE), причем превосходство это довольно значительное: на середину 2014

г. iOS всех версий суммарно насчитывает 335 уязвимостей, тогда как Android только 36.

Количество уязвимостей в операционной системе Apple в связи с презентацией бета-версии iOS-8 выросли - появились новые векторы для атаки: сторонние клавиатуры, множество новых API-вызовов (интерфейса программирования приложений) в новом SDK и система управления «умным домом» HomeKit. Несмотря на такое большое количество уязвимостей, пользователям iOS не стоит беспокоиться о своей защищенности, так как Apple, как правило, закрывает новые уязвимости достаточно быстро;

- Google, в свою очередь, также делает упор на усиление безопасности своей операционной системы. В Android версии 4.4 появился модуль SELinux, который в принудительном режиме осуществляет контроль доступа на уровне ядра. Данный модуль работает независимо от базовой модели безопасности Linux.

Таким образом, *в контексте собственной безопасности операционной системы победителем не является ни одна из двух ОС.* И Android, и iOS имеют мощные механизмы защиты от хакерских атак, и обе компании, Google и Apple, уделяют безопасности своих систем повышенное внимание.

8. В последние годы активно растет число пользователей, которые используют свои личные мобильные девайсы для выполнения рабочих задач. Эта тенденция, получившая название BYOD (Bring Your Own Device), несет в себе определенные риски безопасности для корпораций. При помощи уязвимого либо просто утерянного смартфона или планшета злоумышленники могут получить несанкционированный доступ к секретной документации компании либо к ее внутренним ресурсам, например к почте. В связи с этим возникает потребность в использовании решений типа MDM (Mobile Device Management), позволяющих централизованно управлять политиками безопасности мобильных устройств, работающих в сетях компании.

С точки зрения безопасности на уровне корпорации ОС от Apple имеет ряд преимуществ перед Android. iOS имеет в своем арсенале мощные средства для централизованного управления девайсами, такие как профили конфигурации, возможность удаленного полного сброса и встроенная поддержка сторонних MDM-решений. Android в чистом виде таких возможностей не имеет. Для интеграции с MDM-

системами на Android необходимо предварительно устанавливать специальное ПО.

Стоит отдельно отметить, что компания Samsung ушла далеко вперед в вопросах корпоративной безопасности по сравнению с другими производителями устройств на Android. Речь идет о программе SAFE (Samsung For Enterprise) и надстройке KNOX, которая представляет собой хорошо защищенный контейнер для всех рабочих активностей пользователей с поддержкой сторонних MDM-систем.

Все аппараты от Samsung, работающие на Android 4.3 и выше, полностью соответствуют принципам защищенного бизнеса. Тем не менее, Apple имеет гораздо меньшую линейку продуктов, нежели производители Android-устройств, поэтому ей не составляет труда обеспечить поддержку систем корпоративной безопасности для всех своих смартфонов, планшетов и актуальных версий ОС. В категории наиболее безопасной для использования на уровне компаний операционной системы победителем выходит iOS.

Резюмируем основные плюсы и минусы двух операционных систем с точки зрения безопасности:

***Android***

*Плюсы:*

- открытость для исследователей безопасности;
- иммунитет приложений к переполнениям буфера;
- строгий контроль доступа на уровне ядра (SELinux).

*Минусы:*

- большое количество потенциально вредоносного ПО в магазине Google Play;
- слабые возможности в обеспечении корпоративной безопасности;
- большое число версий ОС и моделей девайсов от различных производителей, что усложняет стандартизацию методов защиты.

***iOS***

*Плюсы:*

- тщательный контроль загружаемых в App Store приложений, и, как следствие, практически полное отсутствие вредоносного ПО в магазине приложений;
- быстрая реакция Apple на инциденты безопасности;
- большие возможности по поддержке систем корпоративной безопасности.

*Минусы:*

- большое количество известных уязвимостей в самой операционной системе;
- рост числа возможных векторов для атаки (интеграция в экосистему Apple, система HomeKit).

В заключение можно сказать, что на самом деле сегодня мало кто будет выбирать телефон, учитывая его защищенность как основной критерий. И это правильно, потому что системы Android и iOS по возможностям защиты своих пользователей сегодня находятся на одном уровне.

# ГЛАВА 7. УЯЗВИМОСТИ В МОБИЛЬНЫХ ПРИЛОЖЕНИЯХ

## 7.1. Классификация мобильных приложений

Под мобильными приложениями понимают компьютерные программы, созданные специально для использования в мобильном телефоне, смартфоне или коммуникаторе, которые предназначены для выполнения той или иной задачи.

Существует несколько подходов к классификации приложений для мобильных устройств.

***По способу установки:*** платные и бесплатные.

***По типу контента:*** развлекательные (мультимедийные), коммуникационные, навигационные, справочные и прикладные.

**По способу разработки*:***

- нативные приложения;
- мобильные сайты, веб-приложения;
- гибридные приложения.

*Нативные приложения (Native Apps*). Нативные – это приложения, которые требуют установки. Такие приложения доступны через иконки на экране смартфона. Они устанавливаются через магазин приложений (Google Play или App Store). Разрабатываются специально под конкретную платформу и имеют доступ ко всем функциям устройства - фотокамере, GPS, акселерометру, компасу, списку контактов и т. д. Такие приложения могут использовать систему отправки уведомлений и могут работать в автономном режиме (без доступа к интернету). Это самый ресурсоемкий тип приложений, но при этом он позволяет максимально использовать возможности, предлагаемые каждой конкретной ОС. Нативные приложения выигрывают как по функционалу, так и по скорости работы у других типов мобильных приложений.

*Мобильные сайты/веб-приложения.* Являются самыми распространенными типами приложений для мобильных устройств и представляют собой мини-сайты, которые, во многом похожи на нативные приложения, но отличаются от них. Они запускаются через браузер и написаны на языке HTML5. Пользователи получают доступ к ним тем же путем, как к любому веб-сайту: они проходят по ссылке, а затем устанавливают их на экране, создавая закладку для этой страницы. Веб-приложения оптимальны для стартапов: они

позволяют достичь большого результата за маленькие деньги и в короткие сроки. Еще один плюс мобильного сайта в сравнении с другими типами приложений – это кроссплатформенность.

*Гибридные приложения*. Гибридные приложения являются частично нативными, частично веб-приложениями. Так же, как нативные приложения, они расположены в магазине приложений и имеют доступ ко многим функциям устройства. Как и веб-приложения, они основаны на HTML, с оговоркой, что браузер встроен в приложение.

В *контексте безопасности приложения* можно классифицировать по месту расположения приложения и по типу используемой технологии передачи данных.

*По месту расположения приложения:*

- SIM-приложения – приложение на SIM-карте, написанное в соответствии со стандартом SIM Application Toolkit (STK);
- Web-приложения - специальные версии для Web-сайтов;
- мобильные приложения, разработанные для конкретной ОС.

Мобильные приложения для конкретной ОС разрабатываются с использованием интерфейса прикладного программирования API (application programming interface). API - это набор готовых процедур, функций, структур и констант, предоставляемых приложением (библиотекой, сервисом) или операционной системой для использования во внешних программных продуктах, устанавливаемого в смартфон.

*По типу используемой технологии взаимодействия с сервером:*

- сетевые приложения – используют собственный протокол общения поверх TCP/IP, например HTTP;
- SMS-приложения - приложения на основе SMS (Short Messaging Service);
- приложения для обмена с сервером (в виде коротких текстовых сообщений);
- USSD-приложения - приложения на основе USSD (Unstructured Supplementary Service Data). Сервис основывается на передаче коротких сообщений, схожих с SMS, но имеющих ряд отличий;
- IVR-приложения – приложения, базирующиеся на технологии IVR (Interactive Voice Response). Система основана на заранее записанных голосовых сообщениях и тональном наборе.

## 7.2. Типовые уязвимости мобильных приложений и способы защиты от них

Компании и организации все чаще используют мобильные технологии, чтобы повысить производительность труда сотрудников и эффективность корпоративной системы. Однако хакеры находят новые способы проникновения и получения доступа к конфиденциальной информации через мобильные приложения. Разработчики и пользователи приложений обнаруживают нарушения безопасности мобильных устройств, которые являются результатом неправильной конфигурации мобильных приложений. Речь идет о множестве пробелов в защите приложений, которые существенно снижающие общую безопасность мобильной системы. Это происходит из-за того, что мобильные приложения выходят на рынок без полной проверки кода и конфигурации на безопасность. Поэтому разработчикам и пользователям важно знать о наиболее распространенных уязвимостях мобильных устройств и наиболее совершенных способах повседневной борьбы с ними.

В соответствии с классификацией открытого проекта обеспечения безопасности приложений OWASP (Open Web Application Security Project), выявили 10 основных уязвимостей, которым подвержены мобильные приложения и устройства в целом:

*M1 Обход архитектурных ограничений (Improper Platform Usage)*

Эта категория охватывает злоупотребление особенностями платформы, обхода ограничений или неиспользования систем контроля управления безопасности платформы. Характерно как для платформы Android, для iOS (обход ограничений Touch ID и Keychain) и других мобильных ОС. Затрагивает системы контроля безопасности, которые являются частью мобильной операционной системы.

*Рекомендации.* В серверной части мобильного приложения должны применяться безопасные методы написания программного кода и конфигурирования. В частности, API-интерфейс должен надежно проверять идентификацию и полномочия лица, его вызывающего.

*M2 Небезопасное хранение данных (Insecure Data Storage)*

Команды разработчиков исходят из того, что пользователи или вредоносный код не получат доступа к файловой системе мобильного

устройства, где хранится конфиденциальная информация. Однако есть немало способов обхода и проникновения к файловой системе:

- некорректное назначение прав доступа для файлов, которое создаёт приложение. На этапе тестирования разработчики часто некорректно назначают права доступа и забывают редактировать их при финальном выпуске программного продукта, в связи с чем, у злоумышленников появляются возможности для несанкционированного доступа;

- хранение важных данных на SD-карте. Часто пользователи хранят важные данные на SD-карте, забывая, что эти данные доступны для всех приложений по умолчанию;

- логирование. Логи представляют собой файлы регистрации, содержащие записи обо всех событиях, происходящих в мобильной операционной системе. В Android любое приложение при установке может запросить права доступа на чтение логов. Многие пользователи не обращают внимания на этот запрос, но опасность заключается в том, что любое устанавливаемое приложение, которое запросило доступ к чтению логов, и при этом получило одобрение со стороны пользователя, получит право чтения всей информации, которое приложение заносит в логи, если логирование не выключено пользователем. Зачастую в логи попадает вся отладочная информация и персональные данные без шифрования;

- получение прав суперпользователя (администратора). Часто пользователи смартфонов стремятся к получению полного доступа к файловой системе устройства, чтобы обеспечить возможность установки сторонних приложений (не из официальных магазинов AppStore или Google Play Market). На мобильных устройствах компании Apple эта процедура называется Jail Break, а на Android-смартфонах – получение Root-прав (или прав суперпользователя). Стоит отметить, что jail-break или root – это компрометация всей системы безопасности устройства, а не просто опция, расширяющая возможности смартфона.

*Рекомендации.* Меры, которые следует предпринимать для защиты персональных данных мобильного устройства от несанкционированного доступа:

- не допускать хранения важных данных на SD-карте;

- отключить логирование перед установкой приложений;

- при разработке приложений необходимо настроить права доступа с учетом того, что мобильное устройство пользователя может быть скомпрометировано root-правами;

- периодически просматривать конфигурационные файлы на предмет забытых отладочных строк кода, позволяющих получить несанкционированный доступ к персональным данным. Если же бизнес требует хранения конфиденциальной информации на мобильном устройстве, необходимо шире использовать шифрование.

*М3 Небезопасная передача данных (недостаточная защита на транспортном уровне) (Insecure Communication)*

Недостаточное подтверждение достоверности источников связи, неверные версии SSL, недостаточная проверка согласования, передача чувствительных данных в открытом виде и т.д.

Основные проблемы:

- не используется шифрование при передаче данных (например, использование протокола http вместо https);

- при передаче данных используются самоподписанные сертификаты;

*Рекомендации.* Меры по обеспечению информационной безопасности:

- проверка трафика мобильного приложения;

- использование web-сниффера, который будет анализировать трафик мобильных приложений и проверять, чтобы важные данные уходили в зашифрованном виде по протоколу https;

- использование сертификатов, подписанных доверенными центрами;

- при использовании контент-провайдеров (предоставляющих доступ к файлам или базам данных для других приложений) проверять и прописывать прав доступа.

*М4 Небезопасная аутентификация (Insecure Authentication)*

Концентрируясь на защите данных, часто исходят из типичных случаев применения мобильных приложений и пытаются защитить данные применительно к ним. Но истина в том, что существует множество других ситуаций, когда ваши данные просматривают, копируют, кэшируют, регистрируют, создают снимки экрана и резервные копии.

Эта категория относится к аутентификации конечного пользователя или неверное управление сеансами. Включает следующие пункты:

- анонимная работа с приложением. Требования к защищенности мобильных приложений не такие, как к web-приложениям. Предполагается, что пользователь может работать офлайн, поэтому часто используется онлайн-авторизация с последующим хранением данных в сессионных cookie-файлах. После того как были введены идентификационные данные (логин и пароль) и приложение авторизовало пользователя, оно сохраняет специальный идентификатор, который в дальнейшем предъявляется серверу при каждом запросе, поступающем от приложения. Если злоумышленник получил идентификатор пользователя и при этом в системе не были реализованы процедуры проверки IP-адреса сессии или наличия более одного соединения в пределах сессии, злоумышленник сможет получить доступ в систему с правами аккаунта пользователя;

- слабые пароли. Считается, что в мобильных приложениях пароли не должны быть длинными, и большинство приложений разрешает создавать пароли от четырех символов. При этом пароли в большинстве случаев не шифруются и помещаются в базу в хешированном виде. Если злоумышленник получил доступ к базе данных, то с помощью готовых хэш-таблиц расшифровать пароли из четырех символов для него – тривиальная задача, требующая незначительных временных затрат.

*Рекомендации.* Меры защиты при данном типе уязвимости:

- аутентификация в мобильном приложении должна соответствовать таковой в web-версии;

- локальная аутентификация должна работать через cookie файлы только после авторизации на сервере;

- создание сложных паролей длиной более 6 символов.

- контролировать устройства с помощью решения для управления мобильными устройствами (mobile-device management, MDM) или мобильными приложениями (mobile-application management, MAM).

*M5 Слабая криптографическая стойкость (Insufficient Cryptography).*

Мобильное приложение может включать или использовать алгоритм шифрования/дешифрования, который слаб по своей природе и может быть напрямую вскрыт враждебными силами из-за того, что разработанная архитектура имеет принципиальные изъяны или процессы управления ключами плохо организованы.

*Рекомендации.* Необходимо применять более сложные процедуры криптографические процедуры защиты информации.

*M6 Небезопасная авторизация (Insecure Authorization)*

Категория описывает недостатки авторизации (проверка (валидация) на стороне клиента, принудительный просмотр и т.д.). Такие события отличаются от проблем аутентификации (например, устройства регистрации, идентификации пользователей и т.д.).

*Рекомендации.* Приложение должно проходит проверку подлинности пользователей (например, не предоставлять анонимный доступ к некоторым ресурсам или службам без проверки подлинности и запрета несанкционированного доступа).

*M7 Контроль содержимого клиентских приложений (Client Code Quality)*

Проблема заключается в особенностях реализации технологий написания программного кода в клиент-сайд приложениях, отличающиеся от написания кода и его реализации в сервер-сайд приложениях. К ним относятся: переполнение буфера, format string уязвимости, а также другие ошибки на уровне кода. Решением является необходимость переписать код, который работает на мобильном устройстве.

Широко распространено заблуждение, будто вредоносный код не может изменять мобильные приложения (например, подменять библиотеки или внедрять код в приложения).

*Рекомендации.* Защитите приложения от взлома, как в статичном состоянии, так и во время исполнения. Производите проверку входных данных приложений и API-интерфейсов, проверяйте целостность конфиденциальной информации и будьте осторожны при использовании WebView, поскольку это может создать уязвимости вроде межсайтового скриптинга (XSS).

*M8 Модификация данных (Code Tampering)*

Эта категория описывает изменение исполняемых файлов, локальных ресурсов, перехват вызовов сторонних процессов, подмена runtime методов и динамическую модификацию памяти.

После установки приложения, его код остается резидентным в памяти устройства. Это позволяет зловредному приложению изменять код, содержимое памяти, изменять или заменять системные методы API, изменять данные и ресурсы приложения. Все это может обеспечить злоумышленнику возможность манипулирования

сторонними приложениями для совершения нелегитимных действий, кражи данных или извлечения иной финансовой выгоды.

*Рекомендации.* Никогда не исходите из того, что этим источникам данных можно доверять, и должным образом защитите их от фальсификаций и злоупотреблений, в т. ч. с использованием аутентификации, авторизации, проверок целостности, шифрования или других механизмов.

*M9 Анализ исходного кода (Reverse Engineering)*

Атакующие могут использовать учетные данные сессии при аутентификации для доступа к серверным сервисам и осуществлять действия от имени конкретного пользователя.

*Рекомендации.* Применяйте механизм ограничения времени действия cookie для сессий, как на сервере, так и на клиенте. В общем случае рекомендуется ограничить время одним часом или менее. Проследите, чтобы ваш сервер открывал новую сессию для каждого пользователя всякий раз, когда требуется аутентификация. Убедитесь, что на сервере прежние сессии уничтожаются/объявляются недействительными для предотвращения повторного использования.

*M10 Скрытый функционал (Extraneous Functionality)*

Часто разработчики включают в код приложений скрытые функциональные возможности, бэкдоры или другие механизмы, функциональность которых предназначена для общего использования. Под эту категорию подходит известное определение "security through obscurity" (безопасность через непонятность). В устах хакера это означает практикуемый многими продавцами операционных систем стиль, который заключается в продаже системы с оставленными в ней дырами в системе безопасности. Естественно, об этих дырах нет ни слова в документации, что позволяет продавцам считать, что их вроде бы и нет вообще. При этом они наивно верят, что никто из покупателей не сможет их обнаружить. Но такие дыры не могут долго оставаться незамеченными, и рано или поздно всегда найдется хакер, которому захочется воспользоваться такой дырой.

*Рекомендации.* Особенности защиты приложений зависят от характера угроз и от мобильной платформы. Для того чтобы приложения были защищены в процессе исполнения, необходима проверка целостности, которая может предотвратить модификацию ресурсов и исходного кода.

# ГЛАВА 8. ТЕХНОЛОГИИ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ БЕСПРОВОДНЫХ И МОБИЛЬНЫХ СЕТЕЙ

## 8.1. Базовый стандарт для беспроводных и мобильных сетей

Существует множество технологий, призванных повысить сетевую безопасность. Все они предлагают решения для важнейших компонентов политики в области защиты данных: аутентификации, поддержания целостности данных и активной проверки.

Под аутентификацией подразумевается аутентификация пользователя или конечного устройства (хост клиента, сервер, коммутатор, маршрутизатор, межсетевой экран и т.д.) и его местоположения с последующей авторизацией пользователей и конечных устройств.

Целостность данных включает такие структуры как безопасность сетевой инфраструктуры, безопасность периметра и конфиденциальность данных.

Активная проверка помогает удостовериться в том, что установленная политика в области безопасности выдерживается на практике, и отследить все аномальные случаи и попытки несанкционированного доступа.

Для обеспечения передачи информации в беспроводных и мобильных сетях базовым стандартом является IEEE 802.11 (Wi-Fi 802.11), который является набором протоколов для передачи данных (transfer).

Стандарт IEEE 802.11 с традиционной безопасностью (Tradition Security Network, TSN) предусматривает два механизма аутентификации беспроводных клиентов:

- открытую аутентификацию (Open Authentication);
- аутентификацию с общим ключом (Shared Key Authentication).

*Открытая аутентификация* не позволяет точке доступа определить, разрешен ли клиенту доступ к сети или нет. Это становится уязвимым местом в системе безопасности в том случае, если в беспроводной или мобильной сети не используется так называемое WEP-шифрование.

Стандарт IEEE 802.11 требует передачи MAC-адресов клиента и точки радиодоступа в открытом виде. В результате этого в беспроводной сети, использующей аутентификацию по MAC-адресу,

злоумышленник может обмануть метод аутентификации путём подмены своего MAC-адреса на разрешенный.

*Аутентификация с общим ключом* является вторым методом аутентификации стандарта IEEE 802.11. Процесс аутентификации с общим ключом аналогичен процессу открытой аутентификации, но отличается от последнего тем, что метод требует настройки статического ключа шифрования WEP (Wired Equivalent Privacy).

В отличие от проводной сети, аутентификация в стандарте IEEE 802.11 ориентирована на аутентификацию клиентского устройства радиодоступа, а не конкретного клиента как пользователя сетевых ресурсов.

Процесс аутентификации в беспроводной сети IEEE 802.11 проиллюстрирован на рисунке 8.1 и состоит из следующих этапов:

1. Клиент посылает кадр (фрейм) запроса *Probe Request* во все радиоканалы.

2. Каждая точка радиодоступа (Access Point, AP), в зоне радиуса действия которой находится клиент, посылает в ответ фрейм *Probe Response*.

3. Клиент выбирает предпочтительную для него точку радиодоступа и посылает в обслуживаемый ею радиоканал запрос на аутентификацию *Authentication Request*.

4. Точка радиодоступа посылает подтверждение аутентификации *Authentication Reply*.

5. В случае успешной аутентификации клиент посылает точке доступа запрос на соединение (ассоциирование) *Association Request*.

6. Точка доступа посылает в ответ фрейм подтверждения ассоциации *Association Response*.

7. Клиент может теперь осуществлять обмен пользовательским трафиком с точкой радиодоступа.

Разработкой стандартов WiFi 802.11 занимается организация IEEE (Institute of Electrical and Electronic Engineers).

В настоящее время IEEE 802.11 представляет собой группу стандартов, позволяющих осуществлять передачу данных на различных скоростях, частотных диапазонах и с различной степенью сетевой безопасности.

IEEE 802.11a – описывает высокие скорости передачи чем 802.11b. Используются частотные каналы в частотном спектре 5 ГГц. Протокол не совместим с 802.11b.


Рис. 8.1. Аутентификация по стандарту 802.11

IEEE 802.11b – описывает большие скорости передачи и вводит больше технологических ограничений. Этот стандарт широко продвигался со стороны WECA (Wireless Ethernet Compatibility Alliance) и изначально назывался Wi-Fi. Используются частотные каналы в спектре 2.4 ГГц.

IEEE 802.11g – описывает скорости передачи данных эквивалентные 802.11a. Используются частотные каналы в спектре 2.4 ГГц. Протокол совместим с 802.11b.

IEEE 802.11n – самый передовой коммерческий Wi-Fi-стандарт. В 802.11n используются частотные каналы в частотных спектрах WiFi 2.4 ГГц и 5 ГГц. Совместим с 11b/11a/11g. Поддерживаются частотные каналы Wi-Fi шириной 20 МГц и 40 МГц (2 x 20 МГц). Эта радиочастотная технология называется OFDM (Orthogonal frequency-division multiplexing) - мультиплексирование с ортогональным частотным разделением каналов. Используется также технология OFDM MIMO (Multiple Input Multiple Output) - многоантенная передача вплоть до уровня 4 x 4 (4 передатчика и 4 приемника). При этом минимум 2 передатчика на точку доступа и 1 передатчик на пользовательское устройство.

IEEE 802.11i - наиболее защищенный вариант стандарта 802.11.

На смену WEP пришёл стандарт IEEE 802.11i, представляющий собой комплексную систему обеспечения безопасности. Эта система включает в себя системы аутентификации, создания новых ключей для каждой сессии, управления ключами (на базе технологии Remote

Access Dial-In User Service, RADIUS), проверки подлинности пакетов и т.д.

Разработанный стандарт IEEE 802.11i призван расширить возможности протокола IEEE 802.11, предусмотрев средства шифрования передаваемых данных, а также централизованной аутентификации пользователей и рабочих станций.

Организации, участвующие в разработке и продвижении стандартов Wi-Fi (Wi-Fi Alliance и IEEE), анонсировали стандарт WPA (Wi-Fi Protected Access, защищенный доступ Wi-Fi), который стал составной частью стандарта IEEE 802.11i. Он также обеспечивает совместимость оборудования различных производителей.

Новый стандарт безопасности WPA обеспечил уровень безопасности куда больший, чем может предложить WEP, и имеет то преимущество, что программное обеспечение более старого оборудования может быть заменено без внесения аппаратных изменений.

А позже был разработан и утвержден стандарт WPA2, обеспечивающий еще более высокий уровень безопасности, чем первая версия WPA. WPA/WPA2 представляет собой обновленную программу сертификации устройств беспроводной связи. Преимуществами WPA являются усиленная безопасность данных и ужесточенный контроль доступа к беспроводным сетям.

Изначально WPA основывался на протоколе TKIP (Temporal Key Integrity Protocol), использующий метод шифрования RC4. Между тем WPA2 использует новый метод шифрования CCMP (Counter-Mode with CBC-MAC Protocol), основанный на более мощном, чем RC4, алгоритме шифрования AES (Advanced Encryption Standard). Кроме того, в WPA/WPA2 обеспечена поддержка стандартов IEEE 802.1x, протокола EAP (Extensible Authentication Protocol – расширяемый протокол аутентификации) и проверка целостности сообщений MIC (Message Integrity Check). 802.1x - это стандарт, который используется для аутентификации и авторизации пользователей и рабочих станций в сети передачи данных. Благодаря стандарту 802.1x можно предоставить пользователям права доступа к корпоративной сети и ее сервисам в зависимости от группы или занимаемой должности, которой принадлежит тот или иной пользователь.

Wi-Fi Alliance дает следующую формулу для определения сути WPA:

WPA = IEEE 802.1x + TKIP + EAP + MIC

Из этой формулы видно, что WPA, по сути, является суммой нескольких технологий.

WPA может работать в двух режимах: Enterprise (корпоративный) и Pre-Shared Key (персональный).

В первом случае, хранение базы данных и проверка аутентичности по стандарту IEEE 802.1x в больших сетях обычно осуществляются специальным сервером, чаще всего RADIUS.

Во втором случае подразумевается применение WPA всеми категориями пользователей беспроводных сетей, т.е. имеет упрощенный режим, не требующий сложных механизмов. Этот режим называется WPA-PSK (Pre-Shared Key) и предполагает введение одного пароля на каждый узел беспроводной сети (точку доступа, беспроводной маршрутизатор, клиентский адаптер, мост). До тех пор пока пароли совпадают, клиенту будет разрешен доступ в сеть. Можно заметить, что подход с использованием пароля делает WPA-PSK уязвимым для атаки методом подбора, однако этот режим избавляет от путаницы с ключами WEP, заменяя их целостной и четкой системой на основе цифробуквенного пароля.

Другим важным механизмом аутентификации является проверка целостности сообщений MIC (Message Integrity Check). Механизм используют для предотвращения перехвата пакетов данных, содержание которых может быть изменено, а модифицированный пакет вновь передан по сети.

802.11i (WPA2) – это наиболее устойчивое и безопасное решение, предназначенное в первую очередь для больших предприятий, где управление ключами и администрирование были главной головной болью. WPA2 является обязательным условием для всех сертифицированных Wi-Fi устройств.

802.11ac. Новый стандарт Wi-Fi, который работает только в частотной полосе 5 ГГц и обеспечивает значительно большие скорости как на индивидуального клиента Wi-Fi, так и на точку доступа Wi-Fi. Находится в стадии внедрения.

Помимо основных стандартов Wi-Fi 802.11a, b, g, n, существуют и используются дополнительные стандарты для реализации различных сервисных функций (802.11d, 802.11e, 802.11f, 802.11h,

802.11k, 802.11m, 802.11p, 802.11r, 802.11s, 802.11t, 802.11u, 802.11v, 802.11y, 802.11w**).**

Первым *стандартом шифрования данных* в беспроводных сетях стал выше упомянутый протокол WEP. Формат WEP-кадра приведен на рис. 8.2.

Процедура WEP-шифрования выглядит следующим образом. Первоначально передаваемые в пакете данные проверяются на целостность (алгоритм CRC-32) для получения значения контроля целостности (Integrity Check Value, ICV), добавляемого в конец исходного сообщения. Далее генерируется 24-битный вектор инициализации IV (Initialization vector), представляющий собой произвольное число, которое может быть использовано вместе с секретным 40- или 104-битным ключом для шифрования данных. Полученный таким образом 64- или 128-битный ключ и является исходным ключом для генерации псевдослучайного числа, которое используется для шифрования данных. Далее данные смешиваются (шифруются) с помощью логической операции XOR с псевдослучайной ключевой последовательностью, после этого вектор инициализации добавляется в служебное поле кадра.

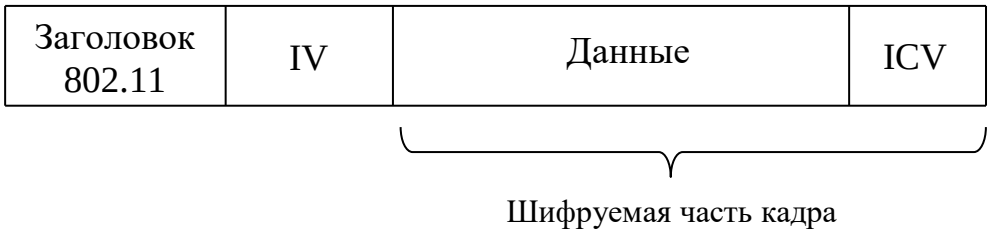



Рис. 8.2. Формат WEP-кадра

Как и любая другая система безопасности на основе паролей, надежность WEP зависит от длины и состава ключа, а также частоты его смены. Первый серьезный недостаток – применение статического ключа – за относительно небольшое время ключ можно подобрать перебором. И второй недостаток WEP-шифрования – самосинхронизация для каждого сообщения, поскольку вектор инициализации передается незашифрованным текстом с каждым пакетом и через небольшой промежуток времени он повторяется. В результате протокол шифрования WEP на основе алгоритма RC4 не является стойким.

Для аутентификации в беспроводных сетях также широко используются два других механизма, которые не являются частью стандарта 802.11, а именно:

- назначение идентификатора беспроводной локальной сети (Service Set Identifier, SSID);
- аутентификация клиента по его MAC-адресу (MAC Address Authentication).

*Назначение идентификатора беспроводной локальной сети (SSID)* представляет собой атрибут беспроводной сети (так называемое имя сети), позволяющий логически отличать сети друг от друга. При попытке пользователя войти в сеть беспроводной адаптер сканирует пространство на предмет наличия в ней беспроводных сетей. При сканировании в режиме скрытого идентификатора сеть не отображается в списке доступных сетей. Подключиться к ней можно только в том случае, если, во-первых, точно известен ее SSID, а во-вторых, заранее создан профиль подключения к этой сети.

Идентификатор SSID регулярно передается точками радиодоступа в специальных фреймах - биконах (beacon) - сигнальных кадрах - одного из наиболее важных фреймов управления. Точка радиодоступа периодически отправляет биконы для анонсирования своего присутствия и предоставления необходимой информации (SSID, частотный канал, временные маркеры для синхронизации устройств по времени, поддерживаемые скорости, возможности QoS - функции обеспечения качества обслуживания и т.п.) всем устройствам в зоне ее покрытия.

Любая приемо-передающая станция, расположенная в радиусе действия и поддерживающая стандарт 802.11, может определить SSID с помощью анализатора трафика протокола 802.11. Некоторые точки радиодоступа позволяют административно запретить широковещательную передачу SSID внутри фреймов-биконах. Однако и в этом случае SSID можно легко определить путем захвата фреймов Probe response frame - фреймов-ответов на полученный фрейм-запрос. Фрейм-ответ содержит информацию о функциональности, поддерживаемых скоростях передачи данных и т.п., посылаемых точками радиодоступа. SSID не обеспечивает конфиденциальность данных. Кроме этого, отключение широковещательной передачи SSID точками радиодоступа может серьёзно отразиться на совместимости оборудования беспроводных

сетей различных производителей при их использовании в одной беспроводной сети.

*Аутентификация клиента по его MAC-адресу*. При аутентификации по MAC-адресу происходит сравнение MAC-адреса клиента либо со списком разрешенных (или запрещенных) адресов клиентов, внесенным в MAC-таблицу точки доступа, либо с помощью внешнего сервера аутентификации (рис. 8.3). Аутентификация по MAC-адресу используется в дополнение к открытой аутентификации для уменьшения вероятности доступа посторонних пользователей.

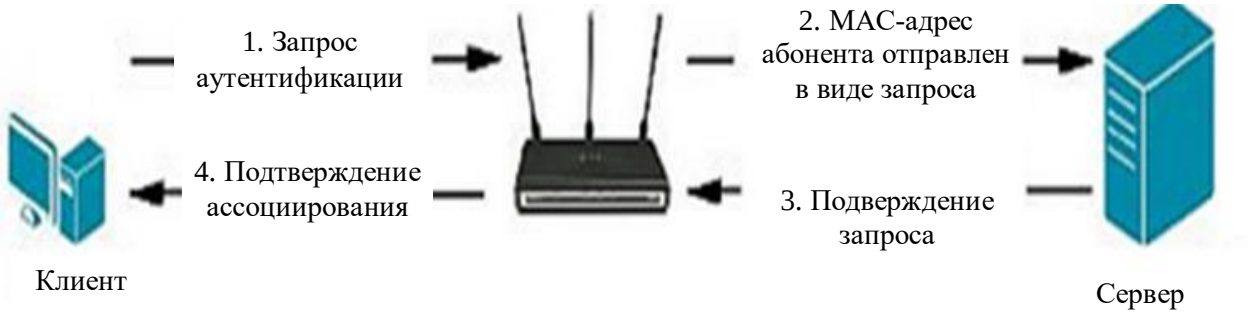



Рис. 8.3. Аутентификация клиента по его MAC-адресу

## 8.2. Стандарты EAP, IEEE 802.1x и IPSec

Проблемы, с которыми столкнулись разработчики и пользователи сетей на основе стандарта IEEE 802.11, вынудили искать новые решения защиты беспроводных сетей.

Были выявлены компоненты, влияющие на системы безопасности беспроводной сети:

- архитектура аутентификации;
- механизм аутентификации;
- механизм обеспечения конфиденциальности и целостности данных.

В связи с этим, был разработан алгоритм "расширяемый протокол аутентификации EAP".

Существует множество версий EAP. Они обычно отличаются сложностью и степенью безопасности выполняемого процесса.

Некоторые процессы обработки запроса на аутентификацию выполняются клиентом, в то время как другие предусматривают двустороннюю аутентификацию клиента и сети. Некоторые

используют шифрование запросов и ответов. Самые распространённые типы EAP – это те, которые встроены в коммутаторы, маршрутизаторы и операционные системы, поскольку их легче всего внедрить.

*Алгоритм аутентификации EAP* (Extensible Authentication Protocol - расширяемый протокол идентификации) - модель идентификации, которая поддерживает множество методов проверки. EAP обычно работает непосредственно на базе протоколов канального уровня типа PPP или IEEE 802 и не требует использования протокола IP.

EAP поддерживает централизованную аутентификацию элементов инфраструктуры беспроводной сети и её пользователей с возможностью динамической генерации ключей шифрования.

EAP может использоваться на выделенных каналах и в коммутируемых устройствах, как в проводных, так и в беспроводных средах. В настоящее время протокол EAP реализован на хостах и маршрутизаторах. Протокол также может быть реализован в коммутаторах и точках доступа, использующих протоколы IEEE-802. Инкапсуляция EAP в проводных средах IEEE 802 описана в стандарте IEEE-802.1x, а инкапсуляция в беспроводных сетях - в стандарте IEEE 802.11i.

Одним из преимуществ архитектуры EAP является ее гибкость. EAP служит для выбора конкретного механизма аутентификации. Механизм аутентификации по протоколу EAP реализуется в два этапа.

Первый этап - пользователь посылает запрос аутентификации аутентифицирующей стороне (например, RADIUS-серверу).

Второй этап - аутентифицирующая сторона запрашивает дополнительную информацию - какой конкретный метод аутентификации использовал пользователь? После получения ответа со стороны пользователя аутентифицирующая сторона дает разрешение авторизироваться и получить права на передачу сетевого трафика.

*Стандарт IEEE 802.1X* используется для аутентификации и авторизации пользователей и рабочих станций в сети передачи данных. Благодаря стандарту 802.1X можно предоставить пользователям права доступа к сети и ее сервисам в зависимости от группы или занимаемой должности, которой принадлежит тот или иной пользователь.

Аутентификация стандарта IEEE 802.1X для беспроводных сетей имеет три главных компонента:

- беспроводной клиент (программное обеспечение клиентского устройства);
- аутентификатор (точка доступа);
- сервер аутентификации (RADIUS).

Защита аутентификации стандарта 802.1x инициирует запрос на аутентификацию от клиента беспроводной сети в точку доступа, которая устанавливает его подлинность через протокол EAP в соответствующем сервере RADIUS. Сервер RADIUS может выполнить аутентификацию пользователя (с помощью пароля или сертификата) или компьютера (с помощью MAC-адреса). Теоретически, клиент беспроводной сети не может войти в сеть до завершения транзакции (рис. 8.4).

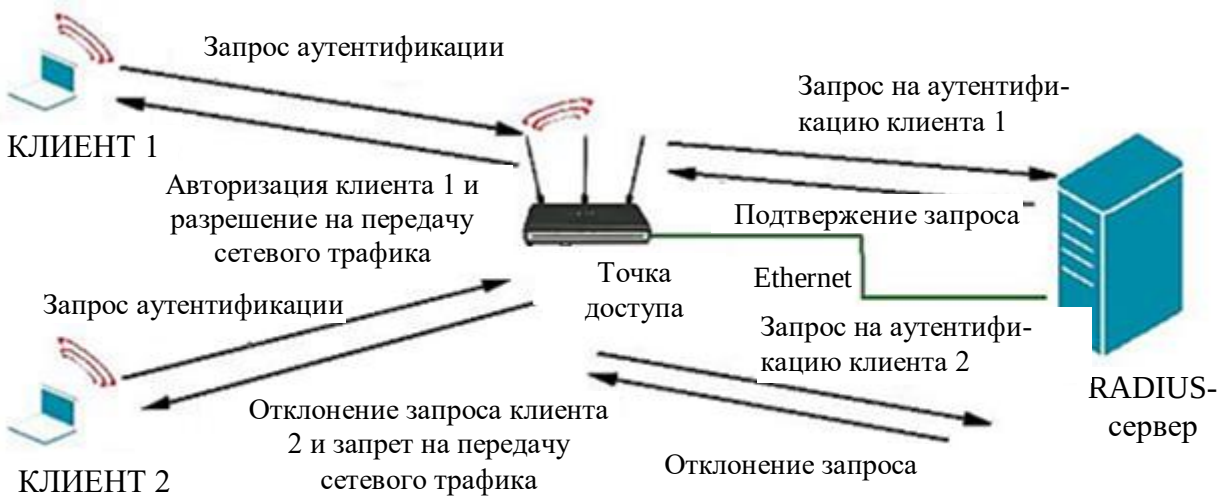



Рис. 8.4. Процесс аутентификации в 802.1x/EAP

IEEE 802.1x предоставляет клиенту беспроводной локальной сети лишь средства передачи атрибутов к серверу аутентификации и допускает использование различных методов и алгоритмов аутентификации. Задачей сервера аутентификации является поддержка требуемых политикой сетевой безопасности методов аутентификации.

Аутентификатор (точка доступа) создаёт логический порт для каждого клиента на основе его идентификатора ассоциирования. Логический порт имеет два канала для обмена данными – неконтролируемый и контролируемый каналы. Неконтролируемый

канал беспрепятственно пропускает трафик из беспроводного сегмента в проводной и обратно, а контролируемый канал требует успешной аутентификации для беспрепятственного прохождения сетевого трафика.

Клиент активизируется и ассоциируется с точкой доступа (или физически подключается к сегменту в случае проводной локальной сети). Аутентификатор распознаёт факт подключения и активизирует логический порт для клиента, сразу переводя его в состояние "неавторизован". В результате этого через клиентский порт возможен обмен лишь трафиком протокола IEEE 802.1x, для всего остального трафика порт заблокирован. Поскольку в локальных сетях IEEE 802.11 нет физических портов, то ассоциация между беспроводным клиентским устройством и точкой доступа считается сетевым портом доступа. Клиент также может (но не обязан) отправить сообщение EAP Start (начало аутентификации EAP) для запуска процесса аутентификации.

После завершения аутентификации сервер отправляет сообщение RADIUS-ACCEPT (принять) или RADIUS-REJECT (отклонить) аутентификатору. При получении сообщения RADIUS-ACCEPT аутентификатор переводит порт клиента в состояние "авторизован", и начинается передача всего трафика пользователя.

В стандарте IEEE 802.1x аутентификация пользователей на канальном уровне выполняется по протоколу EAP. Протокол EAP подобен протоколу CHAP (Challenge Handshake Authentication Protocol – протокол взаимной аутентификации), который применяется в PPP (Point to Point Protocol – протокол соединения "точка-точка"). EAP является "обобщённым" протоколом в системе аутентификации, авторизации и учёта (authentication, authorization and accounting - AAA), обеспечивающим работу разнообразных методов аутентификации.

AAA-клиент (сервер доступа по терминологии AAA в беспроводной сети представлен точкой доступа), поддерживающий EAP. Он может не понимать конкретных методов, используемых клиентом и сетью в процессе аутентификации. Сервер доступа (AAA-клиент) туннелирует сообщения протокола аутентификации, которыми обмениваются клиент и сервер аутентификации. Сервер доступа интересует лишь факт начала и окончания процесса аутентификации.

Есть несколько вариантов EAP, спроектированных с участием различных компаний-производителей (EAP-MD5, EAP-TLS, EAP-LEAP, PEAP). Такое разнообразие вносит дополнительные проблемы совместимости, так что выбор подходящего оборудования и программного обеспечения для беспроводной сети становится непростой задачей.

*Протокол безопасности связи IPSec*

Известно, что на сетевом уровне стека TCP/IP используется протокол IP. Кроме того, в стек TCP/IP входит также протокол безопасной связи IPSec (IP Security – Защищенный IP). Протокол IPSec успешно используется как в проводных, так и в беспроводных (мобильных) сетях.

IPSec выполняет 3 функции:

1. *Аутентификацию и целостность* (гарантирует, что полученный пакет был действительно отправлен стороной, указанной как источник в заголовке пакета, и не был изменен в процессе доставки).

2. *Конфиденциальность* (исключение прочтения передаваемых сообщений третьей стороной).

3. *Управление ключами* (средства управления ключами должны гарантировать защищенный обмен ключами).

Главное свойство IPSec, которое позволяет этому протоколу поддерживать самые разнообразные соединения, является возможность шифрования и/или аутентификации всего потока обмена данными на уровне IP. Таким образом, защита может быть обеспечена любому распределенному соединению, включая удаленную регистрацию, клиент-серверное приложение, электронную почту, передачу файлов, доступ к WEB и т.д.

IPSec обеспечивает защиту любых пакетов, передаваемых протоколами верхних уровней. Согласно модели OSI, протоколам верхних уровней не требуется знать особенности функционирования протоколов, расположенных ниже. IPSec взаимодействует только с прикладным уровнем стека протоколов TCP/IP. Поэтому, любое приложение, поддерживающее работу со стеком протоколов TCP/IP, может использовать протокол IPSec. Это отличает протокол IPSec от всех других подобных технологий (например, механизма SSL - Secure Socket Layer), которые требуют использование соответствующих программных интерфейсов.

Защита на канальном уровне имеет ряд недостатков (сложность конфигурирования, управления ключами, небольшой набор реализуемых функций безопасности). Оптимальное соотношение между прозрачностью и качеством защиты достигается при *формировании защищенных виртуальных каналов (VPN-каналов) на сетевом уровне* (рис. 8.5).

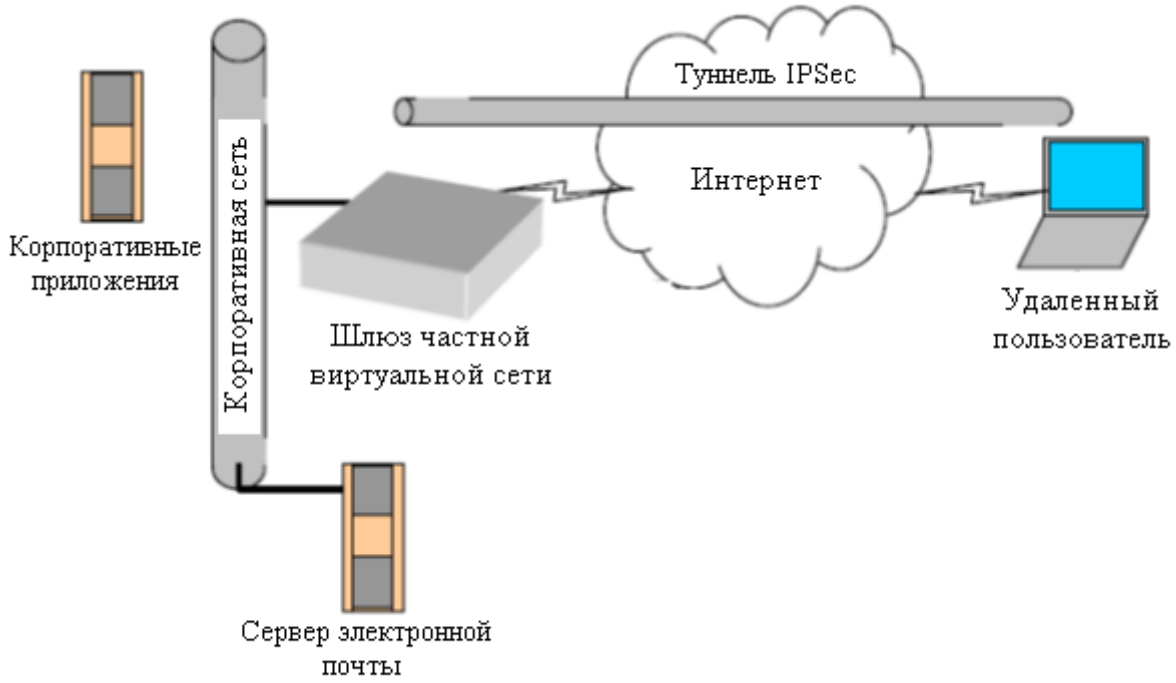



Рис. 8.5. IPSec VPN-туннель

# ГЛАВА 9. ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ В МОБИЛЬНОЙ КОММЕРЦИИ

## 9.1. Модели мобильных финансовых услуг

Современная система оплаты посредством мобильных платежей строиться в основном по схеме, приведенной на рисунке 9.1.

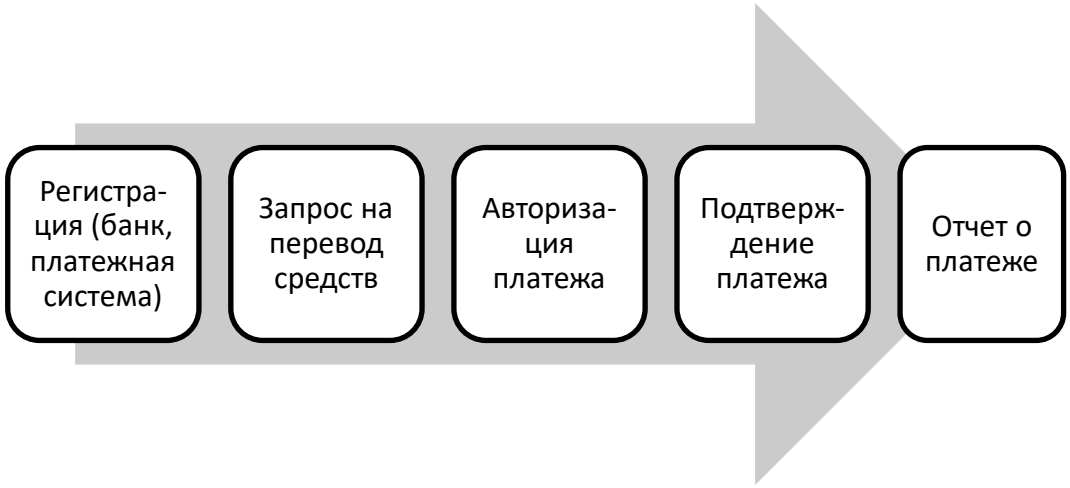



Рис. 9.1. Схема осуществления мобильных финансовых услуг

В настоящее время существуют различные модели финансовых услуг:

- платежи на базе Premium-SMS;
- мобильная коммерция;

***Платежи на базе Premium-SMS*** - это отдельно тарифицируемый тип SMS, используемый для получения каких-либо платных услуг. Premium-SMS сейчас являются наиболее распространённым типом оплаты в различных сервисах мобильных финансовых услуг.

Для оплаты абонент отправляет сообщение на короткий номер оператора, оператор перечисляет со счета абонента необходимую сумму денег (предварительно убедившись, что на счете достаточно средств для осуществления операции) продавцу, после чего абонент получает доступ к сайту или код для активации услуги.

Сообщение оплачивается по специальному тарифу при отправлении (обычно существенно дороже стоимости стандартного SMS). Платеж может инициировать как сам абонент (отправив SMS или запрос через сайт), так и получатель средств - в этом случае требуется подтверждение абонента. После отправки и списания

средств с лицевого счёта, абонент получает доступ к услуге. Иногда Premium-SMS используются и для сервисов, не имеющих прямого отношения к мобильной связи, например, для оплаты в Интернет-ресурсах, для различных голосований и т.д.

Схема выполнения SMS платежей представлена на рисунке 9.2.

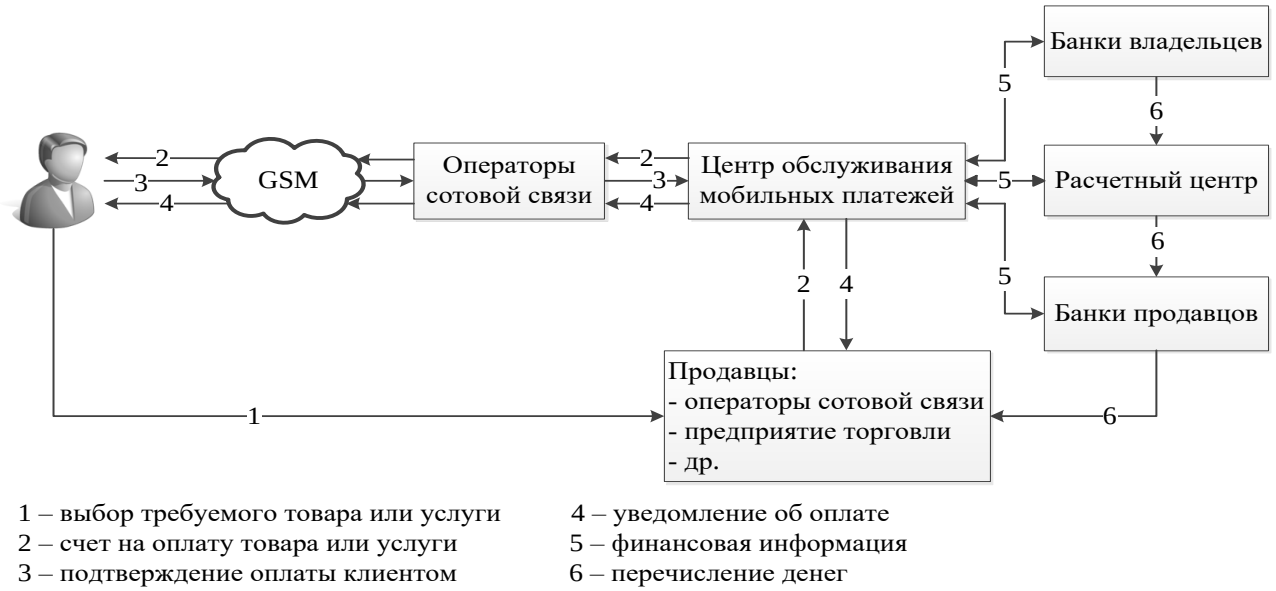



Рис. 9.2. Схема выполнения SMS платежей

В такой модели существует два вида тарификации:

- *MO-тарификация ("Mobile Originated").* Стоимость списывается со счёта абонента в момент отправки SMS-сообщения на определенный короткий номер;

- *MT-тарификация ("Mobile Terminated").* Стоимость списывается со счёта абонента в момент получения SMS-сообщения. Сначала пользователь отсылает SMS на короткий номер (деньги за это не взимаются), затем проверяется, достаточно ли у абонента денег, чтобы оплатить услугу, и готов ли продавец данную услугу предоставить. Если все хорошо, то абоненту отсылается сообщение, за которое и взимается плата.

Плюсы такого способа платежа – пользователю нет необходимости вводить свои личные данные на сайте продавца, не требуется регистрация в какой-либо платежной системе, удобен при спонтанной покупке. Занимает минимальное количество времени для осуществления покупки. Также в плюсе остается и сам оператор, который имеет с этого 30-60% комиссии.

Какой именно вид тарификации используется в конкретном случае, зависит от страны, оператора, короткого номера.

***Мобильная коммерция (mCommerce)*** – общее название для различных коммерческих сервисов, использующих мобильный телефон в качестве основного интерфейса пользователя.

Разница с Premium-SMS заключается в том, что возможно оплаты произвольной суммы платежа в широком диапазоне, тогда как при оплате через Premium-SMS тариф на оплату жестко привязан к короткому номеру.

Процесс осуществляется с помощью карманных компьютеров или смартфонов через удаленное (Интернет, GPRS и т.д.) соединение. Мобильная коммерция, представляет собой смесь Premium-SMS и оплаты с помощью пластиковой карты, реализованная в программно-аппаратном решении по автоматизации процессов взаимодействия с удаленными пользователями. От Premium-SMS технология унаследовала работу через SMS, а от пластиковых карт свободу в выборе суммы платежа и инструменты по отслеживанию его статуса.

Мобильная коммерция объединила в себе передовые технологии мобильной связи и подразделяется на два направления:

- *мобильный банкинг* - при осуществлении платежных транзакций используются денежные средства, находящиеся на банковском счете, управлять которым можно с помощью мобильного телефона;

- *мобильный платеж* - осуществляется без использования банковских счетов пользователя и доступны абонентам, не имеющим собственного банковского счета.

*Мобильный банкинг* – это система, дающая возможность получения информации и управления средствами на банковском счете с помощью мобильного телефона.

В банке при подключении услуги "*мобильный банк*" пользователю предоставляется возможность распоряжаться средствами, находящимися на его банковском счете, с помощью мобильного телефона. Пользователь может пополнить свой счет на мобильном устройстве, счет другого абонента, перевести средства со своего банковского счета на банковский счет другого пользователя. Также есть услуга автоматического пополнения счета мобильного телефона. Необходимо лишь отправить SMS с суммой порога, при достижении которого счет мобильного оператора будет пополнен автоматически.

*Преимущества использования мобильного банкинга*:

- *доступность.* Мобильные устройства есть у всех, а значит услугой может пользоваться каждый;

- *простота в использовании.* Не нужно обладать какими-то специфическими знаниями, чтобы совершить платеж или перевод;

- *экономическая выгода.* Тарифы на использования данного рода услугами значительно ниже, чем при физическом посещении банка.

- *дополнительная информация.* Мобильный банкинг – это не только возможность делать различные платежи. Это еще и отличная возможность получать различного рода информационные услуги.

*Недостатки использования мобильного банкинга*:

- *самой большой угрозой безопасности в мобильном банкинге является* незашифрованность серверов провайдеров сотовой телефонной связи. *Хакер-эксперт сможет сравнительно легко получить информацию о счете или дебетовых и кредитных картах пользователей;*

- *сообщения, полученные от банков, не шифруются.* Это означает, что эту информацию можно легко перехватить при передаче через оператора мобильной связи;

- если мобильный телефон будет украден, информация, хранимая в сообщениях, может быть легко использована другим лицом;

- мобильные телефоны, которые используют интернет-браузеры, но не имеют антивирусной защиты, подвержены очень высокому риску взлома конфиденциальной информации.

С ростом спроса на смартфоны и появлением возможности доступа к высокоскоростному Интернету через сотовый телефон, мобильный банкинг стал следующим очевидным технологическим шагом. Вне всякого сомнения, он обеспечивает комфортный и беспроблемный доступ к счетам. Но с точки зрения информационной безопасности он определенно оставляет желать лучшего. Поэтому до тех пор, пока банки не придумали 100% безопасный способ мобильного банкинга, лучше пользоваться им в самых крайних случаях, когда это абсолютно необходимо.

*Мобильный платёж* - это операция с денежными средствами, осуществлённая с помощью устройства мобильной телекоммуникационной сети. Это платеж с сотового телефона, осуществляемый как через лицевой счет абонента, так и через банковскую карту, который дает возможность оплачивать широкий

спектр услуг - услуги связи, штрафы, коммунальные платежи, кредиты, проезд в общественном транспорте, авиа, ж/д билеты, оплата в точках розничной торговли и на автозаправочных станциях (рис. 9.3).

По способу реализации мобильные платежи бывают *удаленные* и *бесконтактные (см. NFC (Near Field Communication).*

*Удаленные мобильные платежи.* Телефон используется как средство для организации удаленного доступа клиента к его счету. В качестве счета клиента используются счет клиента в биллинговой системе его оператора. Удаленные платежи - система мобильной коммерции, обрабатывающая операции электронной коммерции с поддержкой инфраструктуры беспроводных сетей и беспроводного Интернета. В отличие от систем интернет-платежей, использующих инфраструктуру сети Интернет, беспроводные платёжные системы обрабатывают запросы от мобильных устройств и привязанных к определенному месту терминалов. Эти системы объединяют следующие особенности:


Рис. 9.3. Структура мобильного платежа

- возможность оплаты с помощью мобильного устройства;
- возможности обработки транзакций с помощью POS-терминалов (Point Of Sale - точка продажи) - электронного

программно-техническое устройства для приема к оплате платежных карт, оно может принимать карты с чипом, магнитной полосой и бесконтактные карты), точек обслуживания, географически привязанных транзакций;

- безопасные протоколы беспроводных платежей.

В мобильном платеже могут быть задействованы несколько сторон:

- покупатель, владеющий мобильным устройством, и оплачивающий товары и услуги;
- продавец или поставщик (физическое лицо или организация);
- доверенная третья сторона, осуществляющая аутентификация и авторизацию транзакций, например банк, оператор сотовой связи, оператор кредитных карт;
- поставщик услуг по мобильным платежам. Отвечает за проведение операций.

*Бесконтактные мобильные платежи NFC (Near Field Communication).*

NFC – технология беспроводной высокочастотной связи малого радиуса действия, которая дает возможность обмена данными между устройствами, находящимися на расстоянии около 10 сантиметров.

Преимущества оплаты с помощью NFC:

- возможность совершения покупок в магазинах, оплаты счетов коммунальных услуг, платного телевидения;
- замена наличного расчета на безналичный, в сферах, где ранее это было невозможно (например, оплата проезда в общественном транспорте).

Для использования сервиса NFC необходим встроенный в телефон специальные дополнительные устройства, такие как *NFC-стикеры и NFC-модули.*

*NFC-стикеры* бывают пассивные и активные.

Пассивные NFC-*стикеры* не могут осуществлять обмен данными с мобильным телефоном. Они не дают возможности записи информации в NFC-устройство по каналам связи мобильного оператора (через SMS или через мобильный Интернет).

Активные NFC-*стикеры* используют канал связи Wi-Fi или Bluetooth для связи с телефоном.

В *NFC-модуле* есть микропроцессор, который обеспечивает надежное хранение сервисных приложений, криптографическую защиту и поддерживает три основных канала связи:

- канал NFC для бесконтактных транзакций;

- информационный поток с TSM (Trusted Service Manager), т.е. со службой, которая позволяет поставщикам услуг и мобильным операторам управлять своими бесконтактными приложениями удаленно, обеспечивая доступ к защищенным элементам на терминалах с поддержкой NFC.

- обмен данными с пользователем через мобильное приложение телефона.

*В NFC-модуле записаны сервисные приложения* – программные модули (платежные, транспортные и другие), имеют систему безопасности, защищенные ключами от несанкционированного доступа.

Телефон с *NFC-модулем* устанавливает соединение с платежным терминалом. В результате соединения со счета абонента списывается стоимость услуги.

Существуют три основных области применения NFC:

- *эмуляция карт:* устройство NFC ведет себя как существующая бесконтактная карта;

- *режим считывания:* устройство NFC является активным и считывает пассивную RFID метку, например для интерактивной рекламы;

- *режим P2P* - два устройства NFC вместе связываются и обмениваются информацией.

Возможны и другие способы применений *NFC-модуля:*

- электронная покупка билетов (авиабилеты, билеты на концерт, и другие);

- мобильная покупка билетов в общественном транспорте – расширение существующей бесконтактной инфраструктуры;

- мобильные платежи – устройство действует как платёжная карта;

- электронная доска – мобильный телефон используется для чтения RFID меток, с уличных досок для объявлений, чтобы на ходу получать информацию.

На сегодняшний день услуги по принципу мобильной коммерции предоставляют все операторы Узбекистана.

## 9.2. Уязвимости мобильных платежей и способы защиты от них

Все уязвимости мобильных платежей можно разделить, согласно уровню их реализации, на:

- уязвимости протоколов передачи данных;
- уязвимости технологии передачи (RFID);
- уязвимости мобильной операционной системы;

***Уязвимости протоколов передачи данных.***

Сотовый телефон или "мобильный терминал" подключается к сети оператора через базовые станции. Одна базовая станция обслуживает одновременно несколько мобильных терминалов и является своеобразным "шлюзом", через который проходят голосовые разговоры, интернет данные и другая связанная с конкретным абонентом информация.

В открытом радиоэфире мобильный терминал и базовая станция, предусмотрительно шифруются при помощи специализированных алгоритмов семейства A5. Их несколько:

- A5/0 (без шифрования);
- A5/1 (наиболее массовый, 64-битный ключ);
- A5/2 (слабое шифрование);
- A5/3 (наиболее устойчивый метод, ключ 128 бит).

Проблема в том, что A5/1 и A5/2 были разработаны достаточно давно и с тех пор сильно устарели. Эти схемы шифрования взломаны, а значит, злоумышленник, обладающий определенным специальным программным обеспечением и не слишком дорогой техникой, может перехватывать SMS пользователей прямо из радиоэфира рядом с местом своего нахождения.

Более свежий алгоритм A5/3 считается надежным - подтвержденных случаев его взлома не известно.

Фундаментальная проблема системы безопасности мобильного банкинга связана с тем, что при регистрации в сети аппарат проверяется сетью на принадлежность к ней, а вот сам телефон проверить сеть на адекватность не может, чем успешно и пользуются злоумышленники. Они ставят в непосредственной близости от абонента источник мощного сигнала, маскирующийся под стандартную базовую станцию сотовой сети. Телефон "видит" станцию и, так как сигнал у такой станции более мощный, подключается к ней, такая схема представлена на рис. 9.4.

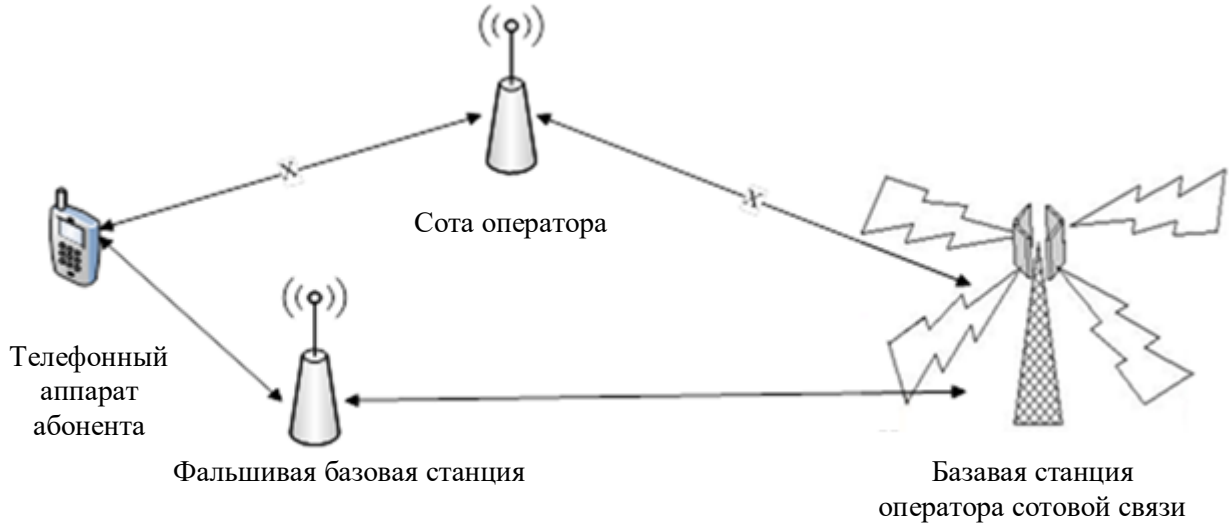



Рис. 9.4. Схема перехвата звонков и сообщений с аппарата абонента

После подключения, станция "командует" телефону перейти на алгоритм A5/0, то есть отключить шифрование, при этом телефон обязан подчиниться. Теперь все разговоры и SMS с него, пока аппарат находится в зоне действия фальшивой базовой станции, в открытом виде проходят через систему злоумышленника. Ничего взламывать не надо: телефон слепо выполняет команды ненастоящей базовой станции и отключает шифрование, а остальное - дело техники.

При таком способе взлома злоумышленник должен всегда находиться в непосредственной близости, чтобы аппарат не подключился к настоящей станции. Фальшивая базовая станция не может принимать входящие SMS и звонки, так как при перенаправлении высвечивается неправильный номер.

В настоящее время большинство сотовых операторов информируют абонента в том, что шифрование отключено специальной пиктограммой или текстом.

Современные 3G- и LTE-сети гораздо лучше защищены от перехвата. Проблемы защиты решаются за счет внедрения новых технологий (алгоритм шифрования A5/3, более защищенные алгоритмы аутентификации, усиление протокола A5/1).

***Уязвимости технологии передачи (RFID)***

RFID – метод автоматической идентификации объектов посредством радиосигналов, в котором считываются и/или

записываются данные, хранящиеся в, так называемых RFID-метках. Любая RFID-система состоит из считывающего устройства (ридер, он же считыватель) и RFID-метки. RFID-метка состоит из двух частей:

- интегральной схемы (микрочипа) для хранения и обработки информации, модулирования и демодулирования радиочастотного сигнала;

- антенны для приема и передачи сигнала.

Сложилось несколько способов систематизации RFID-меток и систем – по рабочей частоте, источнику питания, типу памяти и форм-фактору.

По типу используемой памяти различают следующие RFID-метки:

- *RW (Read and Write)* – такие метки содержат идентификатор и блок памяти для чтения/записи информации. Данные в них могут быть перезаписаны многократно;

- *WORM (Write Once Read Many)* – кроме уникального идентификатора такие метки содержат блок однократно записываемой памяти, которую в дальнейшем можно многократно читать;

- *RO (Read Only)* – данные записываются лишь один раз, при изготовлении. Такие метки пригодны только для идентификации. Никакую новую информацию в них записать нельзя, и их практически невозможно подделать.

Сегодня наиболее широко распространены *пассивные RFID-метки,* не имеющие встроенного источника энергии. Работа такого чипа-метки и передачи ответного сигнала обеспечиваются за счет электротока, индуцируемого в антенне электромагнитным сигналом от считывателя. Пассивные RFID-метки обычно встраиваются в стикер (наклейку на товар в магазине) или имплантируются под кожу. Максимальная дистанция считывания пассивных меток – от 10 см до нескольких метров, в зависимости от выбранной частоты и размеров антенны.

*Активные RFID-метки* имеют собственный источник питания. Соответственно, сигнал с них считывается на большом расстоянии, а сами чипы имеют большие размеры и могут оснащаться дополнительной электроникой.

Активные метки более надежны, чем пассивные, так как в них используются особые сессии связи между меткой и считывателем. Кроме того, активные метки за счет собственного источника питания,

дают выходной сигнал большего уровня, чем пассивные. Это позволяет применять их в воде, теле людей и животных, металлах (корабельные контейнеры, автомобили), для больших расстояний на воздухе. Активные метки более дороги в производстве и имеют большие размеры.

*Преимущества технологии передачи RFID:*

- *возможность перезаписи.* Хранящиеся в RFID-чипах данные могут многократно перезаписываться и дополняться, тем самым сохраняя свою актуальность;

- *большой объем хранимых данных.* RFID-метка может хранить во много раз больше информации, чем штрих-код. На чипе площадью в 1 см2 может храниться до 10000 байт информации, в то время как штриховые коды могут вместить единицы байт;

- *нет нужды в прямой видимости.* В отличие от штрих-кода, взаимная ориентация метки и считывателя не играет роли – метке достаточно ненадолго попасть в зону регистрации, перемещаясь, в том числе и на довольно большой скорости. Метки могут считываться сквозь упаковку, что позволяет размещать их скрытно;

- *большое расстояние чтения.* RFID-метка может считываться на значительно большем расстоянии, чем штрих-код. В зависимости от модели метки и считывателя, радиус считывания может составлять до нескольких сотен метров;

- *устойчивость к воздействию внешних факторов.* Специальные RFID-метки обладают значительной прочностью и сопротивляемостью жестким условиям рабочей среды. В тех сферах применения, где один и тот же объект может использоваться множество раз, радиочастотная метка оказывается экономически самым выгодным средством идентификации. А пассивные RFID-метки и вовсе имеют практически неограниченный срок эксплуатации;

- *интеллектуальность.* RFID-метка может не только переносить данные, но и выполнять другие задачи. Данные на метке могут шифроваться. Радиочастотная метка может закрывать паролем операции записи и считывания данных, а также зашифровывать их передачу. В одной метке можно одновременно хранить открытые и закрытые данные.

*Недостатки технологии передачи RFID:*

- сравнительно высокая стоимость системы;

- уязвимость к воздействию электромагнитных помех;

- возможность использования RFID для незаконного сбора информации о людях.

***Уязвимости мобильной операционной системы***

Современные смартфоны имеют целый ряд уязвимостей. Например, недавно обнаружена критическая уязвимость Android-смартфонов на базе процессоров Exynos 4210 и 4412. Было обнаружено, что набор системных библиотек (deviexynos-mem), которые работают с физической памятью устройства, имеют дыру в системе безопасности, используя которую злоумышленник или вредоносное приложение может получить root доступ ко всей физической памяти смартфона.

Имея права root доступа хакер или вирус могут сделать практически что угодно с физической памятью мобильного устройства. Речь идет не только о возможности кражи всех данных, которые хранятся на смартфоне, но и полном форматировании памяти устройства.

Существуют и более хитрые и искусные способы использования root доступа. К примеру, злоумышленник может заставить телефон набирать определенные номера и отправлять сообщения на короткие номера с повышенной тарификацией, и тем самым, просто красть деньги. Также набрав свой номер, злоумышленник сможет слушать все, что происходит вокруг вашего телефона, а установив программный шлюз получит возможность прослушивать ваши звонки. В этом случае мобильный телефон превратиться в "жучок" прослушки и слежки.

Android-смартфоны с модулем NFC также имеют некоторые проблемы безопасности. Эти дыры давали возможность злоумышленникам загружать вредоносные программы на телефоны пользователей в фоновом режиме, используя канал NFC.

Одной из последних уязвимостей, обнаруженных в Android-смартфонах, позволяет любому приложению, имеющему разрешение на доступ в Интернет, собирать и передавать личные данные пользователя, в том числе данные СМС: номера телефонов и зашифрованный текст сообщений.

Помимо программы, собирающей для компании производителя пользовательские данные, в новых прошивках также присутствует приложение, не только имеющее доступ ко всей вышеперечисленной информации, но и способное предоставить её любому неавторизованному пользователю по запросу на локальный порт, при

этом не требуется никаких специальных разрешений, кроме доступа в Интернет. Это разрешение, помимо всего прочего, позволит передать полученные данные куда и кому угодно.

При использовании мобильного телефона как средства оплаты товаров и услуг, рекомендуется придерживаться некоторых правил:

- при получении сообщения, которое содержит ссылку на Интернет-страницу или просьбу отправить сообщение на короткий номер, не выполнять никаких действий, если вы не заказывали товар или услугу;

- перед отправкой сообщения на короткий номер, необходимо уточнить у оператора и на специализированных ресурсах стоимость отправки сообщения;

- перед заказом товара или услуги внимательно читать условия их предоставления, а также информацию, размещенную с символом "*";

- прежде, чем переводить деньги на чужой абонентский счет, необходимо разобраться, кому именно оказывется материальная помощь.

- не участвовать в незнакомых SMS-конкурсах и SMS-розыгрышах;

- не вводить номер своего телефона на подозрительных сайтах;

- при использовании услуги "мобильный перевод" необходимо быть внимательным при наборе номера телефона;

- не передавать телефон в руки третьим лицам;

- выключать Bluetooth и Wi-Fi, если нет необходимости в их использовании.

Рекомендаций при использовании протоколов, технологий, операционных систем и программного обеспечения для передачи данных с мобильного телефона:

- если криптографическая защита передачи данных отключена, большинство операторов оповещают своих абонентов об этом наличием соответствующей иконки на экране телефона. При наличии такой иконки, рекомендуется прекратить использование телефона для звонков, передачи сообщений и выхода в интернет.

- при использовании технологии передачи данных RFID не следует использовать свой телефон для передачи информации через подозрительные считыватели. Модули NFC следует покупать только у специализированых, проверенных производителей.

- для обеспечения защиты операционной системы мобильного телефона первое, что необходимо сделать - установить антивирусное программное обеспечение. Не стоит скачивать его с подозрительных серверов, у каждого производителя мобильных операционных систем, есть Интернет-ресурс с которого можно скачать проверенное программное обеспечение. При этом даже в случае кражи персональных данных можно будет в судебном порядке компенсировать нанесенных материальный ущерб. В 90% случаев скачивая мобильное приложение со стороннего сайта, можно получить вирус или другую вредоносную программу.

- главная "проблема" мобильных платежей – это, собственно, наличие украденного сотового телефона в руках злоумышленника. Для блокирования действий злоумышленника при краже телефона, необходимо незамедлительно заблокировать SIM карту. Также при установленном на украденном мобильном телефоне приложении для операций с мобильным банком, рекомендуется сменить пароль на доступ к мобильному банку.

- следует помнить, что если телефон был взломан мало просто сменить номер, так как номер SIM карты привязан к IMEI идентификатору телефона. Узнав IMEI, злоумышленники смогут обнаружить устройство, какой-бы номер не использовался.

# ГЛАВА 10. МЕТОДЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИИ В ОБЛАЧНЫХ ВЫЧИСЛЕНИЯХ

## 10.1. Архитектура взаимодействия мобильных приложений и облачных вычислительных систем

Облачные вычисления - серверы, хранилища данных, базы данных, сети, программное обеспечение и др. - предоставление вычислительнывх услуг через Интернет ("облако").

Облачные вычисления в упрощенном виде можно представить как браузерное приложение, расположенное на удаленном сервере. Другими словами, "облачные вычисления" - это представление поставщиком удаленных вычислительных ресурсов по запросу потребителя. Для обычного пользователя этого достаточно знаний об облачных вычислениях. На самом же деле, возможности облачных вычислений огромны: это способность небольших организаций и частных лиц конкурировать с очень крупными компаниями, значительная экономия финансовых затрат, экономия энергопотребления в процессе вычислений.

Одно из самых больших преимуществ облачных вычислений является хранение большого объема информации. В качестве примера можно привести предоставление услуг электронной почты в Интернете. Эти почтовые сервисы часто предоставляют пользователям большое хранилище памяти, используя пространство, которое можно найти в облаке, потому что это обходится гораздо дешевле. В результате исключается возможность потери данных. В последние годы во многих крупных банках все чаще говорят о потере важной информации, о неудовлетворенности клиентов. Если бы эта информация хранилась в облачной среде, вероятность потери данных значительно уменьшилась бы.

Использование мобильных приложений является важным фактором в развитии облачных технологий. При применении облачных технологий пользователь может обмениваться информацией и приложениями без капитальных затрат на аппаратные средства и программное обеспечение. Поскольку все вычислительные возможности будут реализованы в облаке, потребности в закупке высокотехнологического обурудования и аппаратных средств не будут. В результате стоимость мобильных устройств для пользователей будут низкими.

На рисунке 10.1 показана архитектура взаимодействия мобильных приложений и облачных вычислительных систем на примере открытой платформы Open Source (Open Source Mobile Cloud Platform).

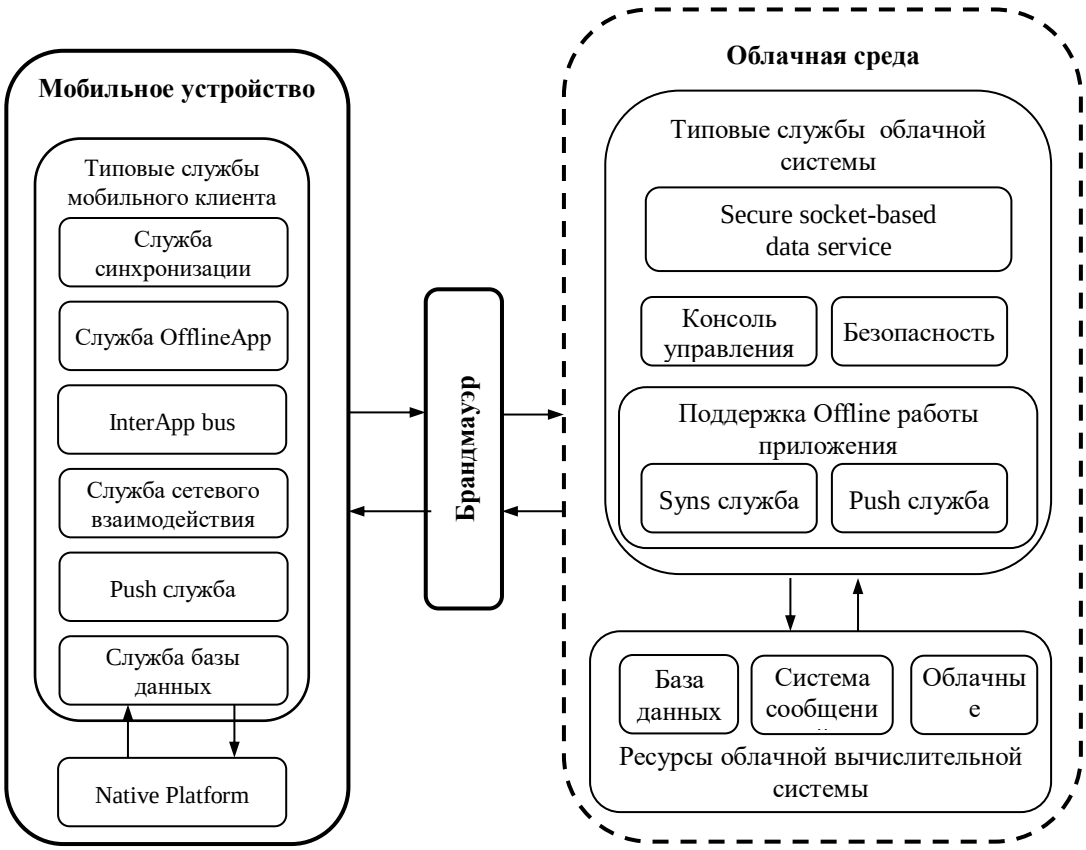



Рис. 10.1. Архитектура платформы OpenMobster

***Типовые службы, необходимые со стороны мобильного устройства:***

*Служба синхронизации* - эта служба передает все изменения, произведенные на мобильном устройстве обратно на облачный сервер.

*Служба OfflineApp* - эта служба позволяет создать координацию в работе низкоуровневых служб, таких как Sync и Push; освобождает программиста от написания кода выполнения синхронизации, поскольку эта служба сама решает, какой механизм синхронизации лучшим образом подходит для данной ситуации. В момент, когда установлен канал передачи данных, push-уведомления и уведомления о синхронизации автоматически обрабатываются Offline App.

*InterApp Bus:* данная служба обеспечивает низкоуровневое взаимодействие между приложениями, установленными на устройстве.

*Служба сетевого взаимодействия* - устанавливает канал передачи, необходимый для получения push-уведомлений от сервера; позволяет автоматически устанавливать связь между устройством и сервером. Это низкоуровневая служба; защищает любое низкоуровневое установление соединения, детали протокола безопасности, благодаря высокому уровню интерфейса платформы.

*Push служба:* управляет обновлениями, рассылаемыми облачным сервисом; улучшает работу пользователя, поскольку пользователю не нужно самостоятельно проверять наличие новой информации.

*Служба базы данных* - представляет собой локальное хранилище данных для мобильных приложений; в зависимости от платформы используются соответствующие возможности для хранения. Основная задача этой службы – хранение и обеспечение безопасного одновременного доступа к данным. Как и Network, является низкоуровневой службой.

***Типовые службы, необходимые со стороны облачной среды:***

*Служба Secure Socket-Based Data Service:* в зависимости от требуемого приложением уровня безопасности эта служба обеспечивает уровень защищенности сокетов (интерфейсов межпроцессорного взаимодействия) простого сокета (plain socket) или SSL socket, т.е. более безопасную связь. SSL socket использует асимметричную криптографию для аутентификации ключей обмена, симметричное шифрование для сохранения конфиденциальности, коды аутентификации сообщений для целостности сообщений.

*Консоль управления* - каждый облачный сервер должен иметь специальное приложение, которое обеспечивает пользователю возможности управления и администрирования системы, например, дистанционное удаление данных, дистанционная блокировка и др.

*Безопасность* - этот компонент обеспечивает аутентификацию и авторизацию, тем самым давая убедиться в том, что подключенные к облачному сервису мобильные устройства действительно имеют к нему доступ. Каждое устройство должно сначала пройти регистрацию. Затем, при активации, устройство проходит процедуру аутентификации/авторизации и лишь потом получает доступ к серверу.

*Sync служба (Cloud Syncronization)* - технология автоматического обновления (синхронизации) данных, расположенных в облачном хранилище (являющейся в данном случае - серверной частью) с данными, расположенными на мобильном устройстве пользователя.

*Push служба* - серверная Push-служба отслеживает каналы передачи данных для обновлений. В момент обнаружения обновлений, соответствующее уведомление отсылается устройству. Если по какой-то причине устройство отключено от сети, служба ожидает и затем, как только устройство подсоединится заново, доставляет уведомление.

## 10.2. Проблемы облачных вычислений в мобильных технологиях и их решения

Облачные вычисления имеют не только плюсы (бесконечная расширяемость объема, низкие издержки использования, низкие инвестиции и риск), но и ряд составляющих необходимых, для предоставления хороших облачных услуг:

− возможность разбиения функций приложения со стороны облака и со стороны устройства;

− низкая латентность сети для более быстрого ответа;

− высокая пропускная способность сети для более быстрой передачи данных между облаком и устройством;

− адаптивный мониторинг состояния сети с целью оптимизации затрат;

− постоянное сетевое соединение для контроля канала;

− возможность поддерживать соединение по запросу;

− иметь возможность выбора сети с учетом энергоэффектиности и низкозатратности.

Данные требования налагают ряд ограничений на использования облачных ресурсов, и приводит к ряду проблем, которые требуют решения:

*Отсутствие открытых общепризнанных стандартов.* Мобильность и взаимодействие между провайдерами облачных услуг невозможны, что затрудняет широкое использование и быстрое развитие облачных технологий. Пользователи с неохотой трансформируют свои текущие источники с данными на облачные

платформы, потому что остается ряд нерешенных технических проблем на этих платформах.

*Ограниченная масштабируемость:* большинство поставщиков облачных услуг заявляют, что они предоставляют бесконечную масштабируемость; на самом деле с широким распространением облачных вычислений и быстрым ростом числа пользователей, никто из поставщиков облачных услуг не в состоянии удовлетворить запросы всех пользователей.

*Ненадежность в доступности услуги:* временные неполадки происходили в работе многих облачных систем, в том числе Amazon, Google, Microsoft. Зависимость от услуг одного поставщика может стать узким местом в случае поломки, так как приложение не может переместиться к другому поставщику облачных услуг, потому услуга просто перестанет предоставляться.

*Блокировка провайдером услуг:* отсутствие мобильности не позволяет приложению и данным перемещаться от одного поставщика облачных услуг к другому.

*Невозможность использования услуг различных облачных систем:* в настоящее время приложения не могут использовать возможности различных облачных вычислительных систем, так как между различными поставщиками облачных услуг нет совместимости.

Возможным решением этих проблем является использование технологии мобильных агентов.

Мобильный агент (МА) - это специальная версия программы Mail.ru Agent для мобильных телефонов. При помощи МА можно поддерживать связь с абонентами, где бы они ни находились.

На сегодня эта программа используется во многих компьютерах, как средство он-лайн общения по всему миру. Она предоставляет возможности как голосовой, так и видео связи, рассылки текстовых сообщений.

МА имеет ряд преимуществ. Помимо общения и рассылки сообщений, эта программа позволяет контролировать трафик, используя возможность своего мобильного оператора. Сама программа абсолютно бесплатна, а деньги списываются со счета только лишь в соответствии с тарифным планом пользователя - это оплата Internet-GPRS трафика.

Кроме того, через МА можно бесплатно отправлять SMS на любые номера из записной книжки вашего телефона. МА позволит

вам сделать "резервную копию" телефонной записной книжки и хранить её на сервере на случай утери аппарата.

Таким образом, МА – это программный модуль, который автономно перемещается между компьютерами в гетерогенной компьютерной сети , взаимодействуя с сервисами на каждой машине для выполнения поставленной пользователем задачи. МА могут быть использованы как посредники между пользователями и техническими устройствами. К примеру, если пользователь хочет управлять устройством, но не обладает соответствующим ПО, он может скачать МА, знающего протокол обмена данными. Исследования в области МА обоснованы на создании с их помощью распределённых систем, обладающих определенными свойствами, такими как: преодоление сетевой задержки, способность к асинхронной и автономной работе, динамичность, кооперативность, живучесть, приложениях для торговли по Интернету, сенсорных сетях и беспроводных сетях.

В настоящее время эта технология привлекает исследователей, работающих в облачных вычислениях, так как она предоставляет решения проблем, существующих в этой области. Исследователи уже осознают, что применение мобильных агентов в этой модели вычислений обеспечивает лучшее решение проблем, преобладающих в этой области.

Как правило, пользовательские запросы посылаются напрямую из облака в Интернет, что приводит к повышению скорости сетевого трафика и уменьшению времени отклика.

Мобильный агент, являясь комбинацией данных и программного обеспечения, которая может мигрировать из одной среды в другую без потери данных, способен выполнять необходимые вычисления в новой облачной среде.

В базовой архитектуре системы представления облачных вычислений с помощью мобильных агентов используется централизованный подход, основанный на Task manager. Каждый административный домен имеет у поставщика облачных услуг свою виртуальную машину и MAP (Mobile Agent Place - место мобильного агента). Одна из виртуальных машин выбирается как task manager, который выполняет множество функций, среди которых – индексация ресурса, аутентификация, безопасность, биллинг, аварийное восстановление, обеспечение отказоустойчивости.

Задача пользователя, представленная в МА как структура данных, отправляется в облако. МАР получает все присланные от мобильного агента данные. МАР информирует Task manager вне зависимости от того, получены или нет данные от мобильного агента. Обмен данными между МАР и Task manager постоянен.

Используя данный мобильно-агентный подход, можно выделить следующую модифицированную архитектуру системы распределения вычислительных ресурсов и выполнения мобильных агентов в облачной среде (рис. 10.2).

Предложенная архитектура способна решить некоторые существующие проблемы совместного использования мобильных технологий и облачных вычислительных систем и дает ряд преимуществ:

*Портативность.* Мобильный агент, передающий код приложения или пользовательские задачи, может перемещаться от одного МАР к другому МАР вне зависимости от специфики облачной системы - тем самым реализуется портативность среди многочисленных облачных вычислительных систем.

*Стандартизация сетевого взаимодействия.* Унификация взаимодействия для различных клиентов и различных вычислительных систем позволяет:

- стабилизировать работу системы при нестабильности сетевого канала;
- нормализировать работу системы при высокой сетевой латентности;
- создать технологический базис для развития эластичных мобильных приложений (Elastic Mobile Applications).

Эластичные (гибкие) мобильные приложения не ограничены возможностями мобильного устройства. Если требуется дополнительная вычислительная мощность или места для хранения, их можно позаимствовать у облака. Сетевое взаимодействие основано на использовании стандартных сетевых протоколов HTTP(S), форматов данных и API. Это дает большую гибкость для устройства.

Эластичные мобильные приложения могут быть запущены на мобильном устройстве или в облаке и могут перемещаться между ними в зависимости от ситуации или предпочтений пользователя.

Архитектура эластичных приложений содержит следующие компоненты (рис 10.3):

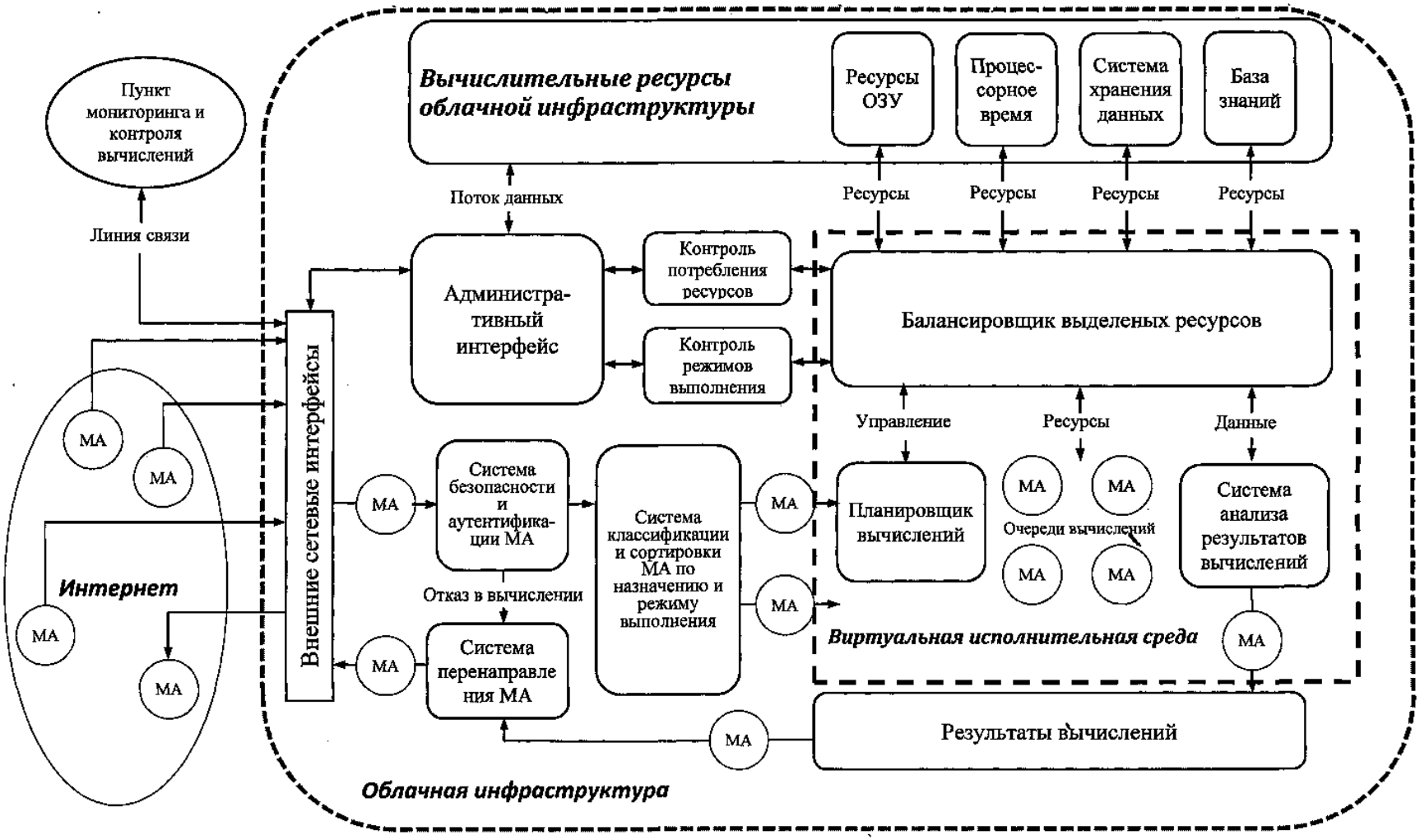



Рис. 10.2. Модифицированная архитектура системы вычисления мобильных агентов в

- *эластичное приложение* – выбирается пользователем и запускается на любой платформе в соответствии с ограничениями мобильного устройства;

- *менеджер эластичности* - запускается на устройстве, контролирует и управляет ресурсами, необходимыми для weblet (программного модуля на языке WIDL - приложение, состоящее из набора функционально независимых и взаимодействующих единиц, называемых веблетами);

- *диспетчер* - принимает решения о том, где протекает процесс: на устройстве или в облаке, запускает оптимизатор для определения энергии, необходимой для weblet, и выбирает оптимальный вариант;

- *маршрутизатор* – промежуточный уровень, получает запросы от пользовательского интерфейса и передает их в веблет; промежуточный уровень необходим, поскольку перемещение веблет должно быть незаметно для пользовательского интерфейса.

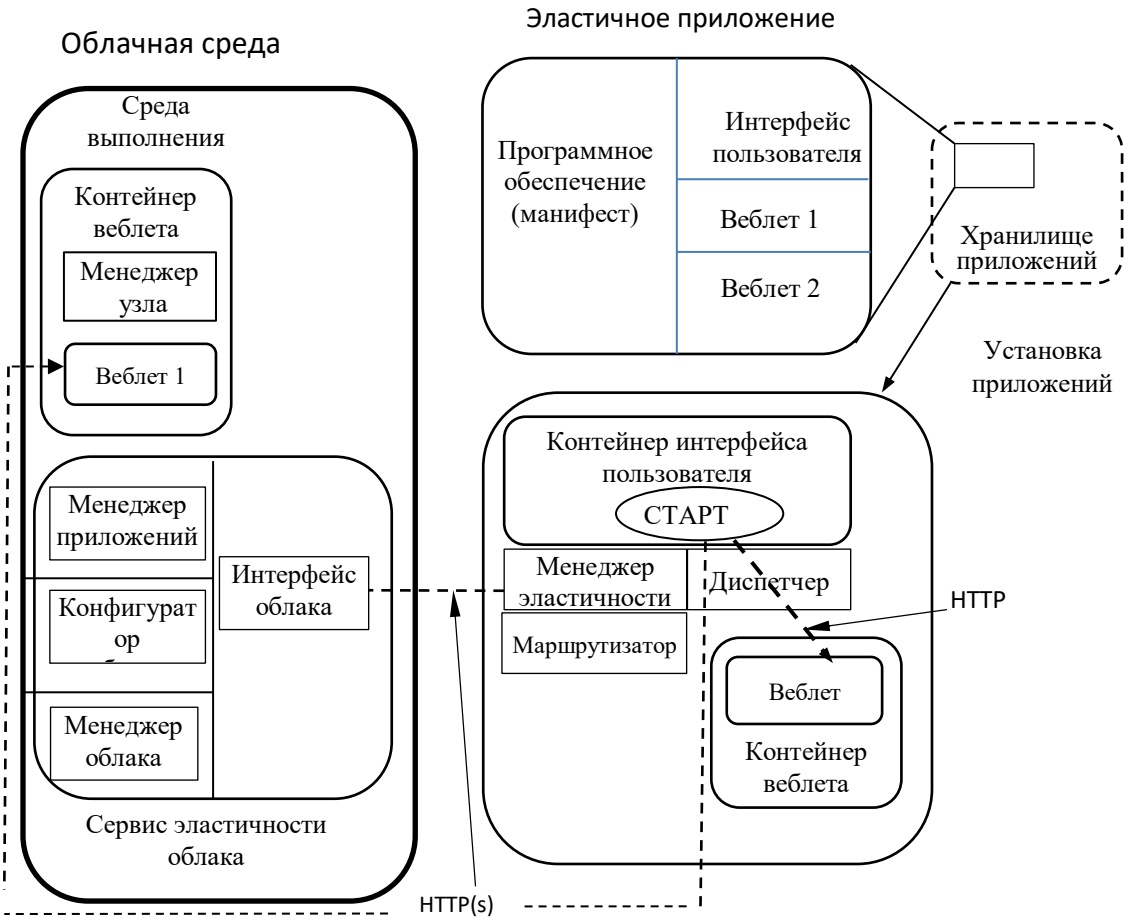



Рис. 10.3. Архитектура эластичных приложений

- *сервис эластичности облака* - распределяет ресурсы к веблетами. Состоит из менеджера приложений, конфигуратора облака и менеджера облака:

- *менеджер приложений* - обеспечивает возможность устанавливать и запускать приложение на мобильном устройстве;

- *менеджер облака* - сохраняет информацию об использовании различных частей приложения, запускаемого на облаке;

- *конфигуратор облака* - осуществляет сбор оперативных данных на облаке;

- *менеджер узла* - работает на каждом узле облака, непосредственно взаимодействует с менеджером приложений и менеджером облака.

Таким образом, концепция облачных вычислений предоставляет новые возможности для развития мобильных приложений, так как перемещают процессы вычислений и обработки в виртуальную среду.

## 10.3. Угрозы облачных вычислений и способы защиты от них

Требования к безопасности облачных вычислений не отличаются от требований безопасности к центрам обработки данных (ЦОД). Однако, виртуализация ЦОД и переход к облачным средам приводят к появлению новых угроз.

Для сохранения целостности данных и обеспечения защиты рассмотрим основные известные угрозы для облачных вычислений.

- *трудности при перемещении обычных серверов в вычислительное облако.* В большинстве традиционных ЦОД доступ инженеров к серверам контролируется на физическом уровне, в облачных средах они работают через Интернет;

- *динамичность виртуальных машин.* Виртуальные машины динамичны. Создать новую машину, остановить ее работу, запустить заново, можно осуществить за короткое время. Они клонируются и могут быть перемещены между физическими серверами. Данная изменчивость трудно влияет на разработку целостности системы безопасности. Однако уязвимости операционой системы или приложений в виртуальной среде распространяются бесконтрольно и часто проявляются после произвольного промежутка времени (например, при восстановлении из резервной копии). В средах облачных вычислениях важно надежно зафиксировать состояние

защиты системы, при этом это не должно зависить от ее состояния и местоположения;

- *уязвимости внутри виртуальной среды.* Серверы облачных вычислений и локальные серверы используют одни и те же операционные системы и приложения. Для облачных систем угроза удаленного взлома или заражения вредоносным ПО высока. Риск для виртуальных систем также высок. Параллельные виртуальные машины увеличивает "атакуемую поверхность". Система обнаружения и предотвращения вторжений должна быть способна обнаруживать вредоносную активность на уровне виртуальных машин, вне зависимости от их расположения в облачной среде;

- *защита бездействующих виртуальных машин.* Когда виртуальная машина выключена, она подвергается опасности заражения. Доступа к хранилищу образов виртуальных машин через сеть достаточно. На выключенной виртуальной машине абсолютно невозможно запустить защитное программное обеспечение. В данном случае дожна быть реализована защита не только внутри каждой виртуальной машины, но и на уровне гипервизора;

- *защита периметра и разграничение сети.* При использовании облачных вычислений периметр сети размывается или исчезает. Это приводит к тому, что защита менее защищенной части сети определяет общий уровень защищенности. Для разграничения сегментов с разными уровнями доверия в облаке виртуальные машины должны сами обеспечивать себя защитой, перемещая сетевой периметр к самой виртуальной машине (рис 10.4.). Корпоративный firewall — основной компонент для внедрения политики информационной безопасности и разграничения сегментов сети, не в состоянии повлиять на серверы, размещенные в облачных средах.

Наиболее эффективными способами обеспечения безопасности "Облачных технологий" являются:

- шифрование;
- защита данных при передаче;
- аутентификация;
- изоляция пользователей.

*Шифрование* – один из самых эффективных способов защиты данных. Провайдер, предоставляющий доступ к данным, должен шифровать информацию клиента, хранящуюся в ЦОД (Центр обработки данных – совокупность серверов, размещенных на одной

площадке с целью повышения эффективности и защищенности), а также в случае отсутствия необходимости, безвозвратно удалять.

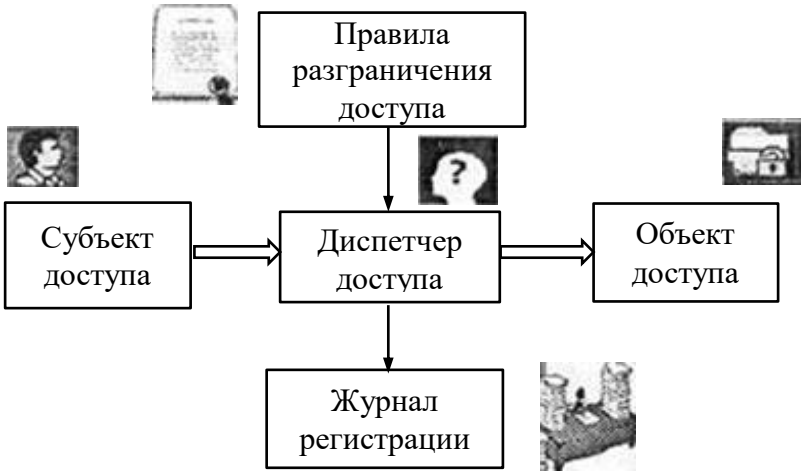



Рис. 10.4. Схема работы механизма разграничения доступа

При шифровании данных всегда возникает вопрос о ключах. Их хранение на облачном сервере нецелесообразно, поскольку каждый, кто имеет доступ к облачным серверам или шаблонам, мог бы получить доступ к ключу, а значит, и к расшифрованным данным. Набор пароля при запуске системы, как это принято в локальных решениях для шифрования данных, затруднен в связи с отсутствием настоящей консоли, однако идея неплоха. Физический ввод ключа заменяется запросом, который облачный сервер отправляет внешнему источнику - серверу управления ключами (Key Management Server, KMS).

Решающим фактором для обеспечения безопасности такого решения является раздельная эксплуатация облачного сервера и сервера управления ключами: если оба размещены у (одного и того же) провайдера облачных сервисов, то вся информация снова оказывается собранной в одном месте (рис. 10.5).

*Защита данных при передаче.* Для безопасной обработки данных обязательным условием является их шифруемая передача. В целях защиты данных в публичном облаке используется туннель виртуальной частной сети (VPN), связывающей клиента и сервер для получения публичных облачных услуг. VPN-туннель способствует безопасным соединениям и позволяет использовать единое имя и пароль для доступа к разным облачным ресурсам. В качестве средства передачи данных в публичных облаках VPN - соединение использует общедоступные ресурсы, такие как Интернет. Процесс

основан на режимах доступа с шифрованием при помощи двух ключей на базе протокола Secure Sockets Layer (SSL).

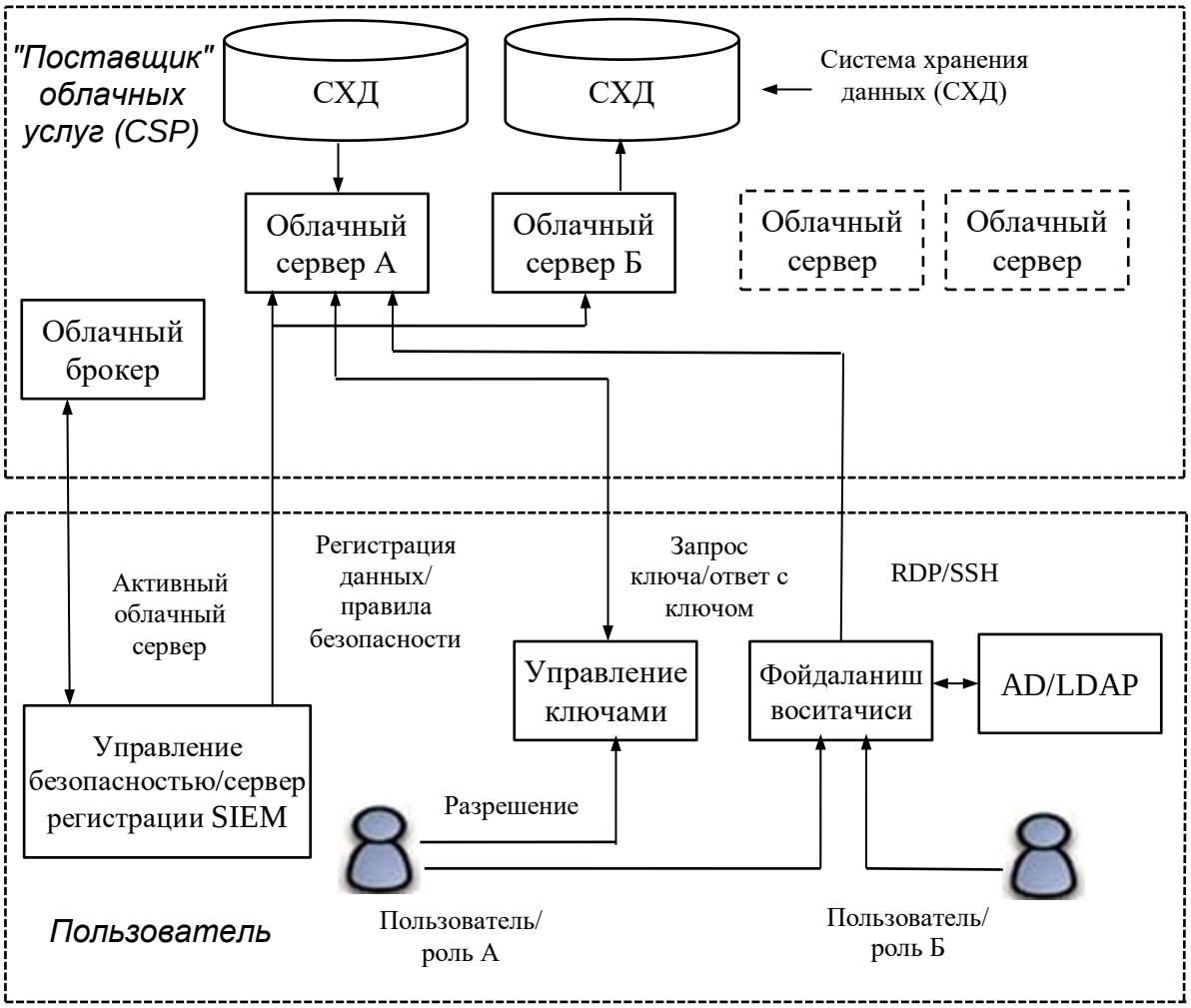



Рис. 10.5. Схема взаимодействия пользователя, сервера управления ключами и облачного сервера. (RDP/SSH - протокол Remote Desktop Protocol (RDP) для связи с сервером через шлюз SSH; LDAP (Lightweight Directory Access Protocol) - "облегченный" протокол доступа к каталогам.

Большинство протоколов SSL и VPN в качестве опции поддерживают использование цифровых сертификатов для аутентификации, посредством которых проверяется идентификационная информация другой стороны, причем еще до начала передачи данных. Такие цифровые сертификаты могут храниться на виртуальных жестких дисках в зашифрованном виде, и используются они только после того, как сервер управления ключами проверит идентификационную информацию и целостность системы. Следовательно, такая цепочка взаимозависимостей позволит передавать данные только тем облачным серверам, которые прошли

предварительную проверку. Зашифрованные данные при передаче должны быть доступны только после аутентификации.

*Аутентификация*. Для обеспечения более высокой надежности, часто прибегают к таким средствам, как токены (электронный ключ для доступа к чему-либо) и сертификаты. Наиболее простой и достаточно надежный метод аутентификации — это технология одноразовых паролей (One Time password, OTP). Такие пароли могут генерироваться либо специальными программами, либо дополнительными устройствами, либо сервисами, с пересылкой пользователю по SMS. Основное отличие облачной инфраструктуры заключается в большой масштабируемости и более широкой географической распределенности. На первый план выходит использование для получения одноразовых паролей мобильных гаджетов, которые сегодня есть практически у каждого. В самом простом случае одноразовый пароль будет сгенерирован специальным сервером аутентификации и выслан в SMS на мобильный телефон пользователя после ввода правильного статического пароля на страницу доступа к облачному сервису. Для прозрачного взаимодействия провайдера с системой идентификации при авторизации, также рекомендуется использовать протокол LDAP (Lightweight Directory Access Protocol) и язык программирования SAML (Security Assertion Markup Language).

*Изоляция пользователей.* Некоторые провайдеры помещают данные всех клиентов в единую программную среду и за счет изменений в ее коде пытаются изолировать данные заказчиков друг от друга. Такой подход опрометчив и ненадежен. Во-первых, злоумышленник может найти брешь в нестандартном коде, который позволит ему получить доступ к данным, которые он не должен видеть. Во-вторых, ошибка в коде может привести к тому, что один клиент случайно «увидит» данные другого. За последнее время встречались и те, и другие случаи. Поэтому для разграничения пользовательских данных применение разных виртуальных машин и виртуальных сетей является более разумным шагом.

И в заключение хочется сказать, что безопасность не всегда обеспечивается только защитой. Она может быть достигнута также соответствующими правилами поведения и взаимодействия объектов, высокой профессиональной подготовкой персонала, безотказностью работы техники, надёжностью всех видов обеспечения функционирования объектов информационной безопасности.

# ГЛАВА 11. АУДИТ И МОНИТОРИНГ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ БЕСПРОВОДНОЙ СЕТИ

## 11.1. Аудит информационной безопасности беспроводной сети

*Аудит беспроводной сети* - процедура, призванная определить текущее состояние беспроводной сети и на основе полученных данных сформировать пакет рекомендаций по ее оптимизации.

В зависимости от целей, аудит беспроводных сетей может различаться масштабами. Незначительные проблемы, можно локализовать малыми усилиями, с помощью собственного персонала компании, в случае же систематической нестабильной работы сети, лучшим выходом будет приглашение сторонних специалистов для комплексного аудита.

Всю процедуру проведения аудита защищенности также можно подразделить на несколько этапов (рис. 11.1):

- анализ беспроводной сети в соответствие с системой критериев оценки защищенности с целью выявления механизмов защиты, реализованных в соответствие со стандартами;
- анализ беспроводной сети с целью выявления дополнительных механизмов защиты информации;
- исследование основных механизмов защиты с целью определения уровня доверия (УД) к беспроводной сети на основе разработанной системы уровней доверия отдельно по криптографическим функциям и функциям аутентификации;
- определение промежуточного уровня доверия к объекту оценки (ОО);
- определение истинного УД к БС (беспроводной сети) с учетом реализованных дополнительных механизмов защиты в ней;
- вычисление экономической целесообразности реализованной системы защиты информации в ОО;
- анализ полученных результатов с целью оценки защищенности БС и при необходимости разработки решений для изменения системы защиты БС в соответствии с требованиями заказчика.

На первом этапе необходимо провести пассивный аудит защищенности сети, который представляет собой исследование ОО и выявление реализованных в нем механизмов защиты информации, исходя из возможностей имеющегося оборудования и целей и задач, которые были поставлены при развертывании БС, при отсутствии

моделирования возможных угроз и атак на ресурсы сети. Всю процедуру желательно проводить по критериям оценки защищенности, так как в дальнейшем это значительно упростит и ускорит процессы определения уровня доверия к сети и построения профиля защиты для нее. Данная рекомендация не является обязательной при выполнении аудита в соответствии с данной методикой.

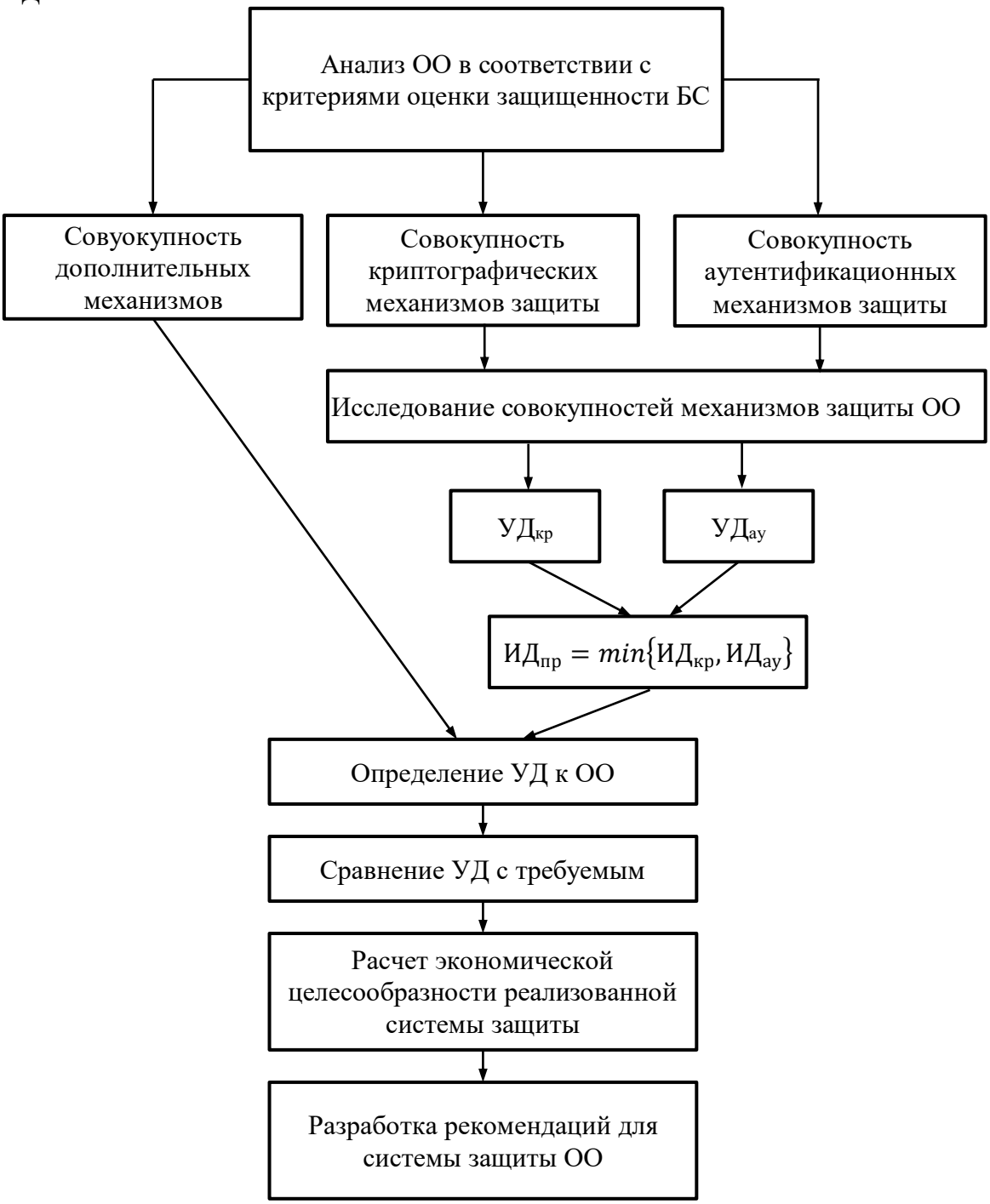



Рис. 11.1. Процесс проведения аудита защищенности беспроводной сети

Второй этап, по сути, представляет собой продолжением первого и является его частью с тем лишь условием, что основное внимание уделяется дополнительным механизмам защиты информации, внедренным в БС в качестве контрмер определенным видам угроз или атак.

На следующем этапе необходимо провести сравнительный анализ полученной совокупности механизмов защиты с целью определения уровня доверия к сети. Как и в случае построения ПЗ для БС, изначально определяется УД по каждой группе механизмов защиты, а потом на основании полученных данных – общий промежуточный УД.

После этого необходимо провести сопоставление полученной совокупности дополнительных механизмов защиты с функциональными требованиями безопасности (ФТБ). Даже, если в дальнейшем не планируется проводить сертификацию либо аттестацию ОО этому процессу стоит уделить должное внимание, так как от точности его результатов во многом зависит определение истинного УД к БС на следующем этапе и в целом корректность суждений об уровне ее защищенности.

После определения истинного УД к БС необходимо сравнить его с тем уровнем, который, по мнению заказчика, должен быть реализован по отношению к объекту оценки. Вполне закономерными являются три возможных результата:

$$УД > УД_{зак};$$
$$УД = УД_{зак};$$
$$УД < УД_{зак};$$

где $УД_{зак}$ - требуемый либо предполагаемый уровень доверия к объекту оценки, по мнению заказчика.

Идеальной представляется ситуация, когда выявленный УД равен тому, которому, по мнению заказчика, и должна соответствовать защищенность БС. Но, к сожалению, вероятность ее незначительна. Зачастую реальный УД ОО не равен предполагаемому. В этом случае необходимо рассчитать экономическую целесообразность реализованной системы защиты.

На основании полученных результатов и в соответствии с требованиями заказчика, можно дать рекомендации по изменению

механизмов защиты, использующих в БС, для соответствия ее требуемому уровню защищенности.

При необходимости усиления либо ослабления системы защиты стоит обратить внимание на уровни доверия, полученные для разных групп механизмов защиты. Вполне возможна ситуация, когда изменению можно будет подвергнуть не всю систему защиты полностью, а только ту ее часть, которая отвечает шифрование передаваемых данных либо за контроль доступа к сети.

## 11.2. Мониторинг безопасности беспроводной сети

Мониторинг безопасности беспроводной сети необходим для обеспечения максимально эффективной работы всех информационных процессов. Проверка сети может быть периодической или разовой. Периодическое обследование сети, как правило, направлено на предотвращение возникновения проблем, в то время как одномоментное обследование делается для того, чтобы сделать выводы: в случае возникновения нежелательных ситуаций в беспроводной сети, моменты возникновения, и при возникновении таких ситуаций - локализация существующих нарушений.

По этой причине различают и "глубину" верификации. Периодическая проверка часто проводится поверхностно, в то время как одноразовая проверка сосредотачивается на максимально подробном аудите неисправностей беспроводной сети.

Может возникнуть необходимость мониторинга на разных этапах развития беспроводной сети. На этапе проектирования исследование радиопомех помогает правильно разместить точку доступа в случае соединения с возможными помехами. Такая проверка может понадобиться и на этапе развития сети (расширения беспроводной сети). Оценка текущего состояния беспроводной сети снимает проблему сдачи в аренду новой точки доступа.

Радиомониторинг беспроводной сети необходим при обеспечении более высокого уровня безопасности беспроводной сети организации.

Ниже, в качестве примера, приводятся сведения о программно-аппаратном комплексе ЗОДИАК, разработаный как специализированный инструмент автоматизированного контроля канала утечки информации по беспроводным сетям.

Возможности программно-аппаратного комплекса ЗОДИАК:

- мониторинг беспроводных сетей в активном и пассивном режимах;

- контроль параметров устройств и соединений в режиме реального времени;

- автоматизированное отслеживание параметров "опасных" сочетаний устройств;

- одновременный мониторинг неограниченного количества устройств и сетей;

- определение скрытых клиентов и точек доступа, которые не видны при программном мониторинге сетевого трафика;

- поддержка многоуровневой сетевой конфигурации;

- определение местоположения обнаруженных устройств.

Мониторинг беспроводных сетей в активном и пассивном режимах:

- пассивный мониторинг пакетов (комплекс только принимает и анализирует пакеты);

- активный поиск, при котором комплекс провоцирует активность "скрытых" клиентов и точек доступа, посылая пакеты специальной формы. В этом режиме комплекс может обнаруживать устройства, "невидимые" в пассивном режиме.

*Контроль параметров устройств и соединений в режиме реального времени.* В режиме реального времени комплекс управляет следующими параметрами:

- определение адреса сетевого адаптера;

- определение имени сети для точки доступа;

- время обнаружения;

- степень активности;

- количество активных соединений;

- режим работы устройства;

- уровни сигналов, поступающих от устройства.

*Автоматизированное отслеживание "опасных" сочетаний параметров устройств.* В комплексе реализовано средство для правильного определения "опасных" сочетаний параметров устройств. Они фиксируют "опасные" сочетания параметров прибора, мониторинг осуществляется в автоматическом режиме и с помощью оператора комплекса. При определении таких параметров, комплекс записывает риски и выполняет заранее установленные действия.

Правила могут быть использованы для настройки фильтрации устройств и ссылок на списки по конкретным наборам параметров. Это дает возможность оптимизировать анализ информации,

например, в случае "неактивности" устройств или "высокого сетевой активности".

*Одновременный мониторинг неограниченного числа устройств и сетей.* В комплексе реализован многорежимный мониторинг и анализ пользовательских пакетов, в том числе скрытых сетей (при условии доступности пароля).

*Определение скрытных клиентов и точек доступа, невидимых программе мониторинга сетевого трафика.* Комплекс принимает и анализирует пакеты данных, поступающих от всех устройств беспроводной сети в зоне радиопередачи. На основе полученной информации составляются комплексные списки активных устройств и перечни их параметров. Анализ полученных пакетов позволяет выявить клиентов сетей и точки доступа не только зоне радиоприема, но в пограничных областях.

*Поддержка многоуровневой сетевой конфигурации.* Информация о структуре сети представляется в виде дерева взаимосвязанных устройств. Это позволяет следить за появлением новых устройств при подключении их в режиме реального времени.

*Определение местоположения обнаруженных устройств.* Для локализации беспроводных сетевых клиентов с разрешением 10 м на крупных объектах, площадях или этажах организуется многозонная конфигурация комплекса.

Зодиак разработан и для того, чтобы идентифицировать технические закладки. По этой причине он позволяет эффективно обнаруживать "опасные" устройства, особенно в условиях высоких нагрузок сигналами от легитимно вещающих устройств.

Зодиак может использоваться как стационарный комплекс при радиомониторинге инфраструктуры беспроводных сетей, так и в качестве мобильного инструмента при проведении специального обследования помещений.

## ИСПОЛЬЗОВАННАЯ ЛИТЕРАТУРА


1. Зубков К. Н., Диасамидзе С. В. Проблемы защиты информации в приложениях для мобильных систем. Ж. Интеллектуальные технологии на транспорте. 2017. № 2.
2. А. С. А. Мутханна, А. А. Атея, М. И. Филимонова. Исследование облачных вычислений в сотовых сетях. Информационные технологии и телекоммуникации. 2017. Т. 5. № 3. Санкт-Петербург.
3. Скабцов Н. "Аудит безопасности информационных систем". Издательский дом "Питер", 2017 г.
4. С.К. Ганиев, М.М.Каримов, З.Т.Худайкулов, М.М.Кадыров. Толковый словарь терминов и понятий по безопасности информации на русском, узбекском и английском языках-Т.: "Iqtisod-moliya" - 2017. 480 с.
5. Сафин Л. К. Исследование информационной защищенности мобильных приложений. Ж. Вопросы кибербезопасности №4(12) - 2015.
6. Безопасность мобильных технологий в корпоративном секторе общие рекомендации. Ассоциация руководителей служб информационной безопасности. Москва, 2015.
7. Лукашов Р. В. «Анализ опыта развития мобильных платежей в мире» ЗАО "Интервэйл", Российская Федерация, 2014 г.
8. Престон Кокс (Preston Cox). Мобильные облачные вычисления: Устройства, тенденции, проблемы и технологии. IBM. Developer Woks. 2014/
9. Мобильные платежи. [Электронный ресурс]. Дата обновления: 03.12.2012. – URL: http://ru.wikipedia.org/Мобильные_платежи (дата обращения: 10.03.2013).
10. Мобильные платежи в контексте СТО БР ИББС и требований по ИБ в НПС. [Электронный ресурс]. Дата обновления: 23.04.2012. – URL: http://slideshare.net/lukatsky/ss-12660626 (дата обращения: 10.03.2013).
11. SMS-платежи: как это работает. [Электронный ресурс]. Дата обновления: 11.02.2013. – URL: http://habrahabr.ru/post/168987/ (дата обращения: 15.03.2013).
12. Мобильная коммерция. [Электронный ресурс]. Дата обновления: 5.05.2011. – URL: http://habrahabr.ru/sandbox/28612/ (дата обращения: 15.03.2013).

13. Бесконтактные платежи. [Электронный ресурс]. Дата обновления: 30.04.2012. – URL: http://habrahabr.ru/company/blog/128564/ (дата обращения: 18.03.2013).

14. Платежи с использованием мобильного телефона. [Электронный ресурс]. Дата обновления: 12.06.2012. – URL: http://mgovservice.ru/technologies/payment/ (дата обращения: 25.03.2013).

15. Мобильный банкинг. [Электронный ресурс]. Дата обновления: 31.08.2011. – URL: http://bankir.ru/publikacii/s/mobilnyi-banking-10000394/ (дата обращения: 16.03.2013).

16. Near Field Communication. [Электронный ресурс]. Дата обновления: 18.04.2012. – URL: http://nfctime.ru/topic/chto-takoe-nfc/ (дата обращения: 18.03.2013).

17. Технология NFC и ее применение. [Электронный ресурс]. Дата обновления: 12.08.2012. – URL: http://rfidsolutions.ru/94.html (дата обращения: 28.03.2013).

18. Взлом сотовых сетей GSM. [Электронный ресурс]. Дата обновления: 9.08.2010. – URL: http://news.tut.by/it/193253.html (дата обращения: 1.04.2013).

19. Радиочастотная идентификация (RFID). [Электронный ресурс]. Дата обновления: 10.04.2013. – URL: http://ru.wikipedia.org/wiki/RFID (дата обращения: 2.04.2013).

20. Уязвимости смартфонов на базе Exynos. [Электронный ресурс]. Дата обновления: 16.11.2012. – URL: http://www.jammer.su/214.html (дата обращения: 9.04.2013).

21. Миноженко А. Евдокимов Д. Анализ безопасности банковских приложений. Ж. Digital Security. 2012.

22. Ю.Р. Акинин, В.Н. Черников, В.Ф. Барабанов. Использование ресурсов облачных вычислительных систем и мобильных агентов при решении задач мобильных технологий. Вестник Воронежского государственного технического университета. 2012. Т.8. № 12. С. 66-68.

23. Степаненко В. Мобильные технологии // Мобильные платежи. – М.: КАРТ БЛАНШ, №5, 2010. – С.4-5

24. Иващук И. Ю. Модель и метод построения семейства профилей защиты для беспроводной сети. Автореферат дисс. канд. Санкт-Петербург. 2010.

25. Багров Е.В. Мониторинг и аудит информационной безопасности на предприятии. Вестник ВолГУ. Серия 10. Вып. 5. 2011.

26. Тужилкин О.В., Чувыкин Б.В. Системы мониторинга на основе беспроводных сетей. Известия ЮФУ. Технические науки. Труды научно-исследовательского института физических измерений. Г. Пенза.

27. С.К. Ғаниев, М.М.Каримов, К.А. Ташев. Ахборот хавфсизлиги. Ўқув қўлланма Т., "Aloqachi", 2008, 382 бет.

28. "Ахборот технологиялари. Ахборот хавфсизлиги. Атамалар ва таърифлар". Узбекистан Давлат стандарта. O'z DSt ISO/IEC 2382-8:2007.

29. В.Г. Олифер. Защита информации при работе в Интернет// Connect. -2002. -№ 11.

30. Н.А. Олифер. Дифференцированная защита трафика средствами IPSec //LAN.-2001.":7R)4; http://www.osp.ru/lan/ 2001/04/ 024.htm.

31. Н.А. Олифер. Протоколы IPSec. //LAN.-2001.-M03; http://www.osp.ru/lan/2001/03/024.htm.

32. Гейер, Джим. Беспроводные сети. Первый шаг: Пер. с англ. - М. : Издательский дом "Вильяме", 2005. –192 с.: ил. – Парал. тит. англ.

33. Спутниковые системы навигации. Учебное пособие. Киев. 2008 г.

34. Максим М. Безопасность беспроводных сетей / Мерритт Максим, Дэвид Поллино ; Пер. с англ. Семенова А. В. - М. : Компания АйТи ; ДМК Пресс, 2004. - 288 с.: ил. - (Информационные технологии для инженеров).

35. Столлингс В. Беспроводные линии связи и сети.: Пер. с англ. – М.: Издательский дом "Вильямс", 2003. – 640 с.

36. Вишневский В., Ляхов А., Портной С., Шахнович И. Широкополосные беспроводные сети передачи информации. - М.:Эко-Трендз, 2005. – 592 с.

37. Григорьев В.А., Лагутенко О.И., Распаев Ю.А. Сети и системы радиодоступа. – М.:Эко-Трендз, 2005. – 384 с.

38. Рошан Педжман, Лиэри Джонатан. Основы построения беспроводных локальных сетей стандарта 802.11.: Пер. с англ. - М.: Издательский дом "Вильямс", 2004. – 304 с.

39. Доступ к беспроводным сетям и безопасность сетей стандарта 802.1X: мифы и факты. Техническое описание. www.flukenetworks.com

40. Расширяемый протокол идентификации (EAP) (Extensible Authentication Protocol (EAP). Энциклопедия сетевых протоколов. www.protocols.ru

41. Н.А. Беляев. Организация безопасных вычислений на распределенных мобильных устройствах. Новосибирский государственный технический университет, Новосибирск.

42. Ле-Бодик Г. Мобильные сообщения: службы и технологии SMS, EMS и MMS / Пер. с англ. – М.: КУДИЦ-ОБРАЗ, 2005. – 448 с.

## Интернет-источники

1. http://www.tayle.com – сайт компании ТАЙЛЕ.

2. http://www.airdata.ru – сайт компании Air Data Communications.

3. http://www.dlink.ru – сайт компании D-LINK.

4. http://wifi-wiki.ru

5. http://www.wireless.bape3.org

6. http://www.alpha-teleport.info – сайт компании alpha-teleport.info.

7. http://www.ixbt.com – информационный портал.

8. http://www.wireless.ru – специализированный портал, посвященный беспроводным технологиям.

9. http://www.umd.ru – сайт компании УМД проект.

10. http://www.ferra.ru – информационный портал.

11. http://ru.wikipedia.org – википедия, русский проект свободной многоязычной энциклопедии.

12. http://pcweek.ru – сайт журнала PCWeek Russian Edition.

13. http://www.thg.ru – Русский Tom's Hardware Guide, информационный портал.