

# Технологии беспроводного доступа

## Оглавление

1. Анализ спектральных характеристик технологии Wi-Fi с использованием программного анализатора спектра Asrylic.....	2
2. Анализ трафика технологии Wi-Fi с использованием анализатора трафика .....	4
3. Исследование электромагнитной обстановки с использованием специализированных программно-аппаратных комплексов .....	7
4. Исследование показателей качества технологии Wi-Fi .....	9

# **1. Анализ спектральных характеристик технологии Wi-Fi с использованием программного анализатора спектра Acrylic**

**Цель работы:** исследование использования радиочастотного спектра нелицензируемого диапазона.

**Задание:**

1. Провести сканирование Wi-Fi сети университета.
2. Определить количество подсетей Wi-Fi в корпоративной сети университета.
3. Определить ближайшие точки доступа Wi-Fi сегмента корпоративной сети
4. Определить паразитные точки (например, раздачу Wi-Fi с мобильного телефона).
5. Провести анализ использования радиочастотного спектра в диапазоне 2,4 и 5 ГГц. Сделать вывод о взаимном влиянии точек доступа в корпоративной сети.
6. Сделать вывод об используемых в Wi-Fi сегменте корпоративной сети методах защиты информации.
7. Провести аналогичные исследования в домашней сети. Разработать рекомендации о методах улучшения помеховой обстановки.

## **Методические указания:**

Для выполнения лабораторной работы рекомендуется использовать свободное программное обеспечение. Для выполнения данной работы используется Acrylic WiFi Home (<https://www.acrylicwifi.com/ru/>), использующий в качестве операционной системы Windows. Факультативно также можно воспользоваться анализаторами Wi-Fi сетей для ОС Android.

При проведении исследований Wi-Fi сегмента корпоративной сети обратите внимание, что используются непересекающиеся каналы 1, 6 и 11. Это позволяет уменьшить негативные явления, такие как межканальная интерференция и интермодуляция, которые могут возникать при работе передающих устройств на соседних каналах. В домашней сети нет элементов планирования, часто используется агрегация каналов, поэтому может наблюдаться неоптимальное использование радиочастотного спектра (например, рис.1), что приводит к ухудшению качества передачи данных. Агрегированные каналы обозначаются как сумма двух, например, 1+5.

Чтобы открыть вкладки с масками спектра нужно нажать меню программы в правом верхнем углу и включить функцию Advanced Mode (рис.2).

Обратите внимание, если ваше устройство устаревшей модели, то оно может не работать в диапазоне 5 ГГц. Тогда в соответствующей вкладке вы не увидите отображения спектра.

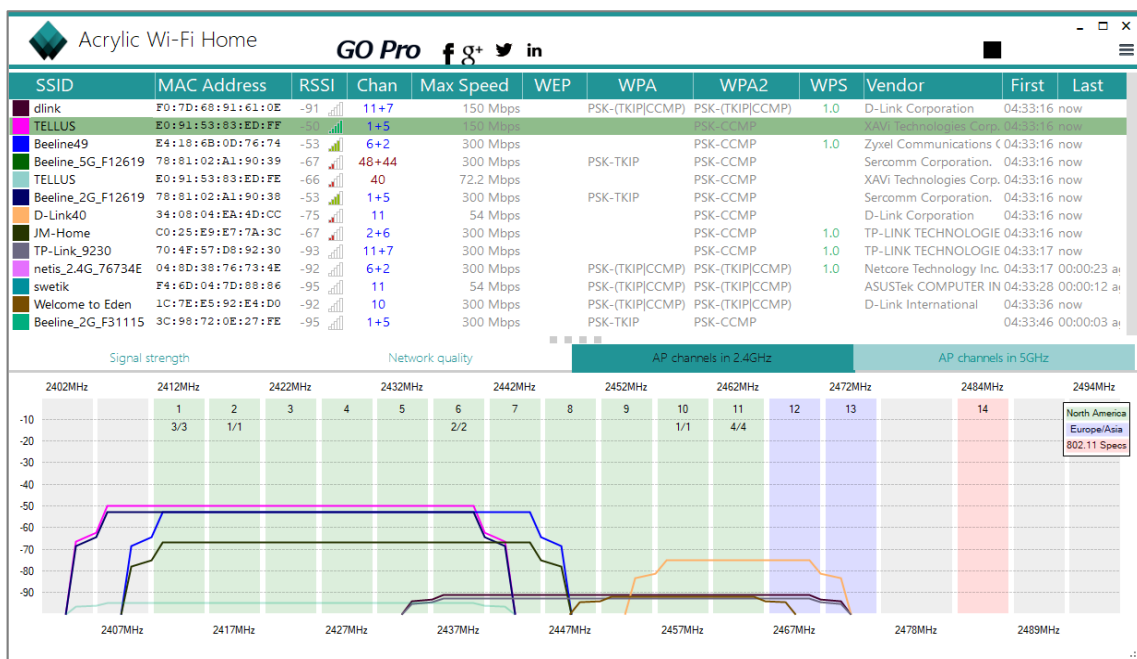


Рис. 1 – Использование частотного диапазона 2,4 ГГц в домашней сети

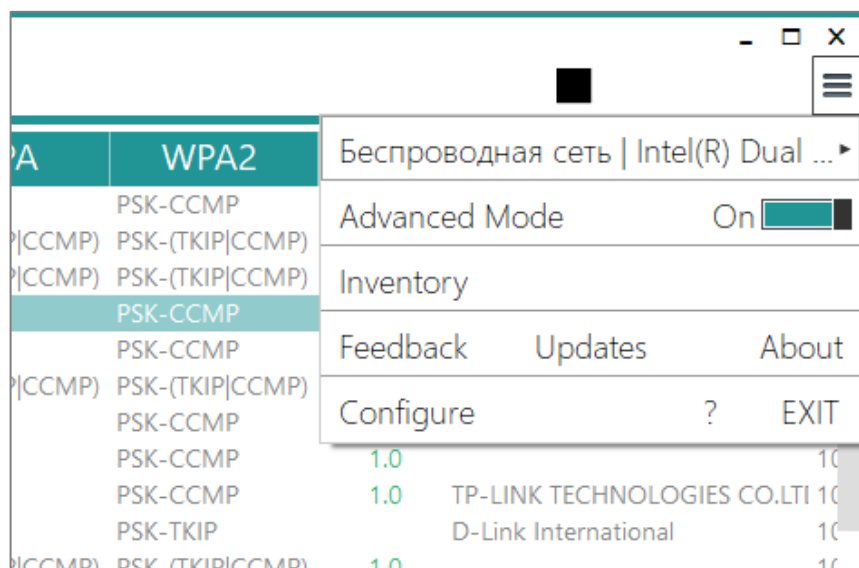


Рис.2 – Включение режима просмотра спектра

**К защите:** в отчете необходимо привести скриншоты корпоративной и домашней сетей и развернутый анализ использования радиочастотного спектра в диапазонах 2,4 и 5 ГГц, а также рекомендации по частотному разнесу.

## 2. Анализ трафика технологии Wi-Fi с использованием анализатора трафика

**Цель работы:** исследование параметров используемых стандартов в сети Wi-Fi.

**Задание:**

**Важно:** все исследования проводятся на реальной сети Wi-Fi.

1. Запустить анализатор трафика WireShark. Выбрать подключение по беспроводной сети Wi-Fi.

*Примечание:* в программе WireShark данная функция доступна только в варианте для OS Linux. Для исследования можно также использовать ПО CommView в ознакомительном режиме.

2. Выбрать пакет L2, принадлежащий к трафику данных, раскрыть его поля (рис.1). Провести анализ выбранного пакета согласно стандарту, описать каждое из полей и данные, которые в нем содержатся.

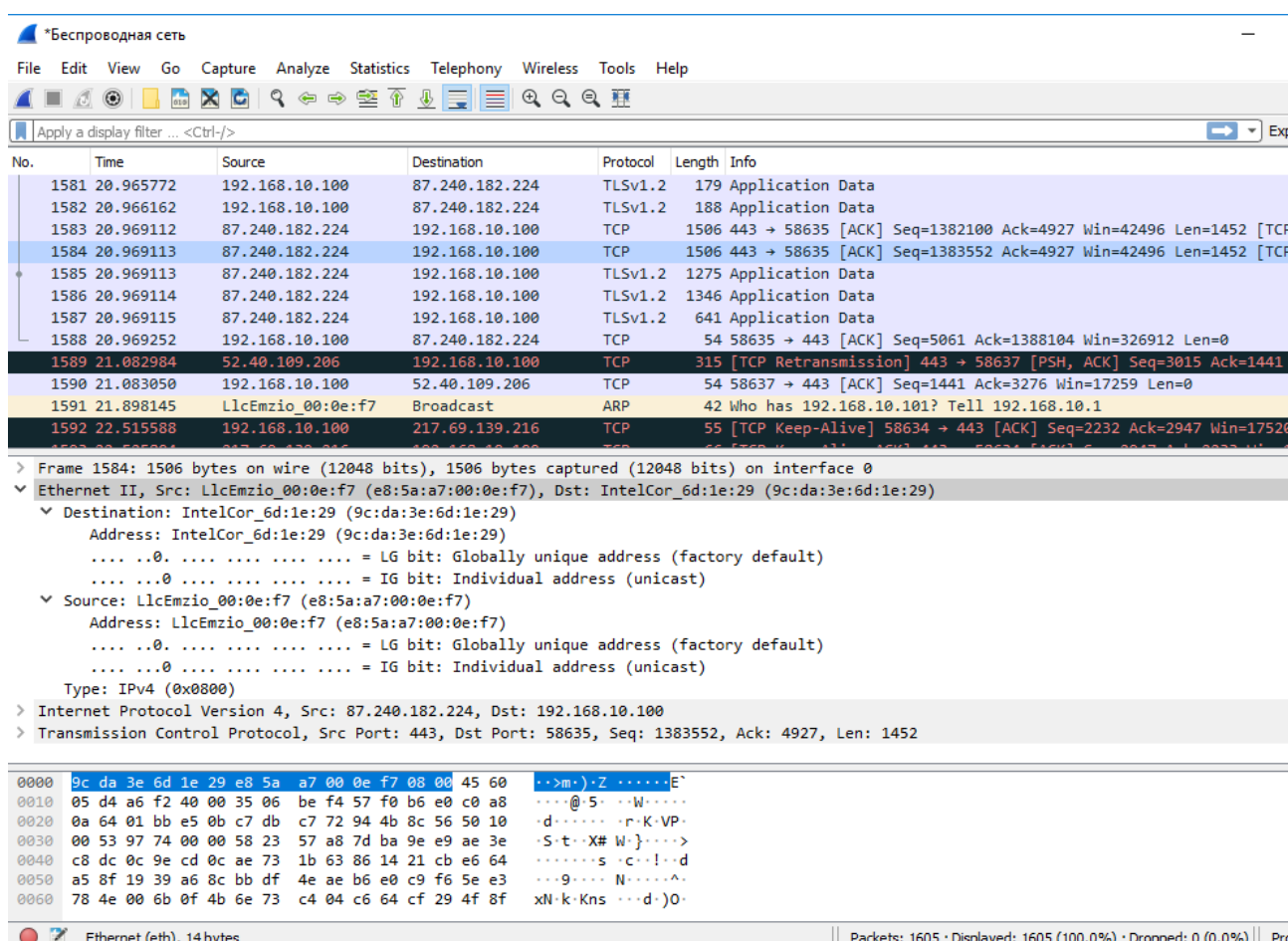


Рис. 1 – Окно WireShark и пакет Wi-Fi, на верхнем уровне – TCP

3. Выбрать управляющие фреймы и раскрыть их поля (рис 2).
4. Выбрать вкладку *Wireless* → *WLAN traffic*. Провести наблюдения за работой Wi-Fi сегмента (время наблюдения 10 минут). Провести анализ работы Wi-Fi сегмента (рис.3).

a)

b)

c)

```

Wireless Packet Info
Signal level: 16%
Signal level in dBm: -76
Noise level in dBm: -90
Rate: 11.0 Mbps
Band: 2.4 GHz
Channel: 11 - 2462 MHz
Date: 5-май-2015
Time: 13:25:42,065007
Delta: 0,011999
Frame size: 204 bytes
Frame number: 2
802.11
  Frame Control: 0x0080 (128)
    Protocol version: 0
    To DS: 0
    From DS: 0
    More Fragments: 0
    Retry: 0
    Power Management: 0
    More Data: 0
    Protected Frame: 0
    Order: 0
    Type: 0 - Management
    Subtype: 8 - Beacon
    Duration: 0x0000 (0)
    Destination Address: FF:FF:FF:FF:FF:FF
    Source Address: 00:22:BE:92:84:24
    BSS ID: 00:22:BE:92:84:24
    Fragment Number: 0x0000 (0)

```

```

Sequence Number: 0x0951 (2385)
Beacon
  Timestamp: 107.622623 sec
  Beacon Interval: 0x0064 (100) - 102.4
  Capability Information: 0x0431 (1073)
    ESS: 1
    IBSS: 0
    CF-Pollable: 0
    CF-Poll Request: 0
    Privacy: 1
    Short Preamble: 1
    PBCC: 0
    Channel Agility: 0
    Spectrum management: 0
    QoS: 0
    Short slot: 1
    APSD: 0
    Radio Measurement: 0
    DSSS-OFDM: 0
    Block Ack: 0
    Immediate Block Ack: 0
    SSID: Bonch
  Supported rates
    1 Mbps
    2 Mbps
    5.5 Mbps
    6 Mbps
    9 Mbps
    11 Mbps
    12 Mbps

```

```

18 Mbps
Current Channel: 11 - 2462 MHz
Traffic indication map (TIM): 0x00 (No)
  Tag Number: Traffic indication map
  Tag Length: 4
  DTIM Count: 0
  DTIM Period: 1
  Bitmap Control: 0x0
  Partial Virtual Bitmap: 0x00 (Not fi)
Country Information
  Country String: RU
Information
ERP Information: 0x02 (2)
  Non ERP present: 0
  Use Protection: 1
  Barker Preamble mode: 0
RSN Information Element (802.11i)
  Version: 0x0001 (1)
  Group Key Cipher Suite: 00 0F AC 02
  Pairwise Key Cipher Suite Count: 0x0
  Pairwise Key Cipher Suite List
  Authenticated Key Management Suite
  Authenticated Key Management Suite
  RSN Capabilities: 0x0028 (40)
Extended Supported Rates
  24 Mbps
  36 Mbps
  48 Mbps
  54 Mbps

```

b)

```

Unknown element id: Tag: 133, length:
Unknown element id: Tag: 150, length:
RSN Information Element (WPA)
  Version: 0x0001 (1)
  Group Key Cipher Suite: 00 50 F2 02
  Pairwise Key Cipher Suite Count: 0x0
  Pairwise Key Cipher Suite List
  Authenticated Key Management Suite
  Authenticated Key Management Suite
  RSN Capabilities: 0x0000 (0)
Vendor specific: Cisco Systems, Inc.
  Tag: Vendor Specific
  Length: 6
  OUI: Cisco Systems, Inc.
  OUI Type: 1
  Aironet IE type: Unknown (0x1)
Vendor specific: Cisco Systems, Inc.
  Tag: Vendor Specific
  Length: 5
  OUI: Cisco Systems, Inc.
  OUI Type: 3
  Aironet IE type: Unknown (0x5)
Vendor specific: Cisco Systems, Inc.
  Tag: Vendor Specific
  Length: 5
  OUI: Cisco Systems, Inc.
  OUI Type: 11
  Aironet IE type: Unknown (0x9)

```

e)

```

Vendor specific: Cisco Systems, Inc.
  Tag: Vendor Specific
  Length: 5
  OUI: Cisco Systems, Inc.
  OUI Type: 20
  Aironet IE type: Unknown (0x9)

```

Рис.2 - Раскрытый фрейм MNGT/BEACON

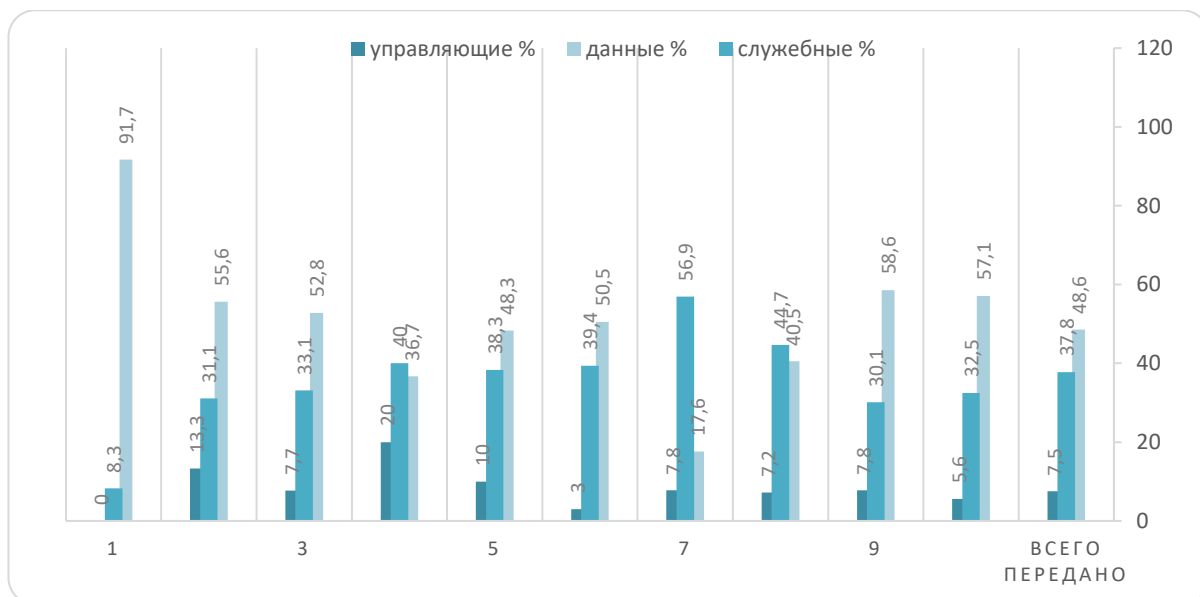


Рис. 3 – Соотношение различных типов трафика в анализируемой сети Wi-Fi

Анализ интенсивности трафика проводят с помощью инструмента *Statistics→IO Graph* (Рисунок 3). Данный инструмент позволяет выбирать до 5 протоколов и обладает возможностью наглядной визуализации. На рисунке 6.3 видно, что трафик имеет пачечную структуру, что характерно для трафика данных и видео по запросу.

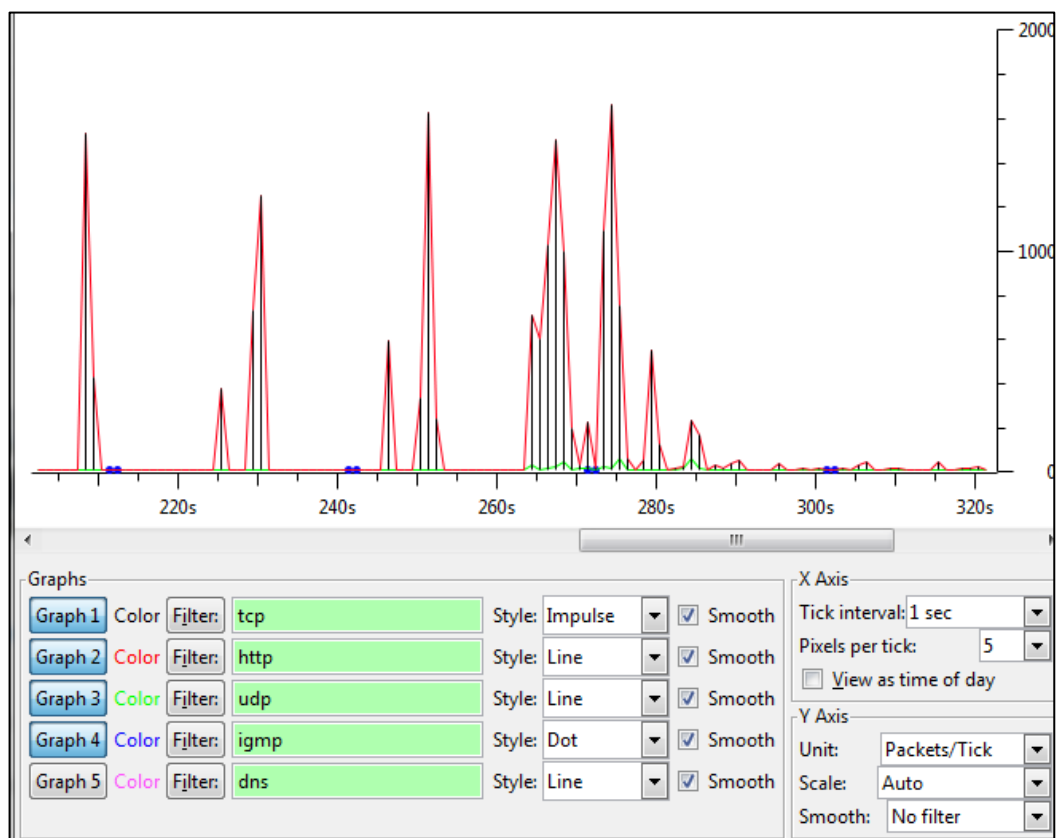


Рисунок 3 – Пример анализа трафика с помощью IO Graph

5. Построить распределение времени поступления фреймов в канал. Выбрать время наблюдения 1с, 400мс, 100мс, 200мс. Графики удобно строить с использованием какого-нибудь табличного редактора (рис. 4). В приведенном примере распределение построено с использованием функции ЧАСТОТА в MSExcel.

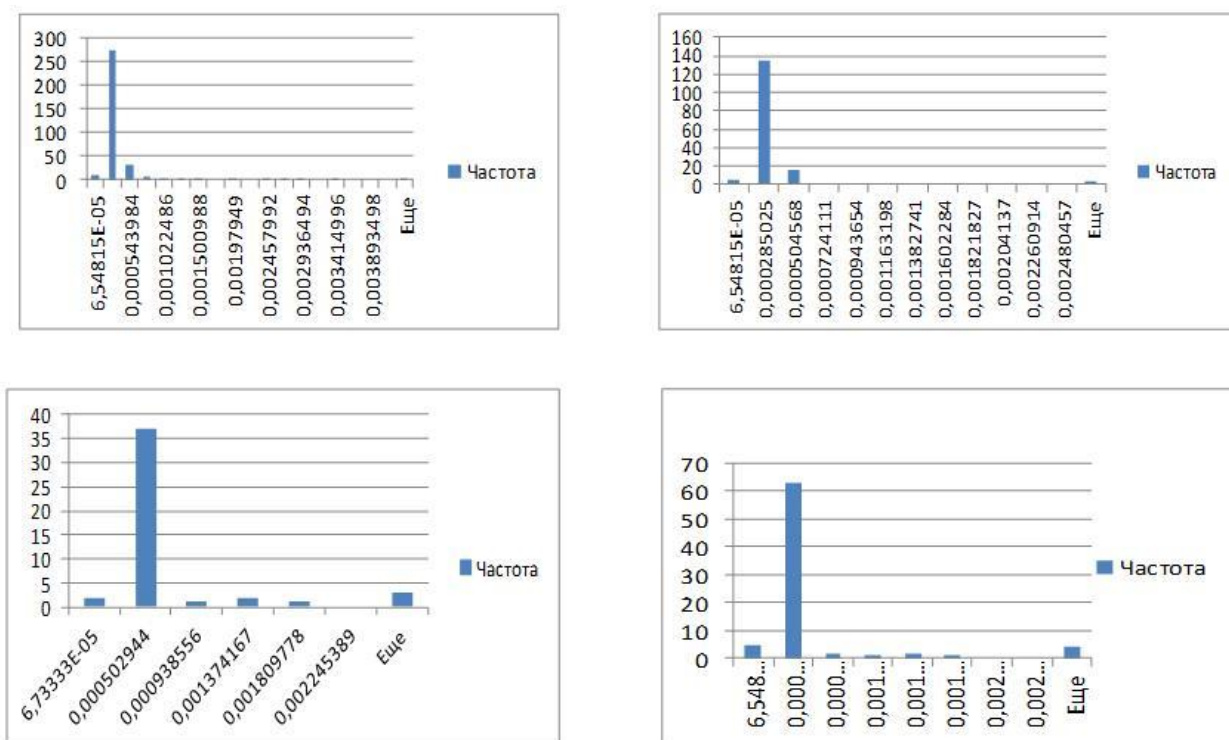


Рис. 4 – Распределение времени поступления фреймов в канал, время наблюдения 1с,400мс, 100мс,200мс соответственно

**К защите:** отчет должен содержать структуру фреймов трех видов (управляющие, служебные, данные), график и анализ соотношения служебного, управляющего и трафика данных в сети в наблюдаемый интервал времени, графики распределения времени поступления фреймов в канал.

### 3. Исследование электромагнитной обстановки с использованием специализированных программно-аппаратных комплексов

**Цель работы:** исследование изменений электромагнитной обстановки с использованием комплекса инспектирования сетей Wi-Fi.

#### Задание:

1. Установите на ноутбук программу TamoGraph Site Survey или Acrylic Wi-Fi Heatmaps. Это программное обеспечение можно использовать в тестовом режиме ограниченное время. Некоторые встроенные сетевые адаптеры не совместимы с данным программным обеспечением, поэтому в этом случае обратитесь к преподавателю и получите совместимый адаптер.
2. Проведите инспектирование Wi-Fi сети на территории университета. При инспектировании необходимо:
  - Загрузить карты (карты университета можно загрузить с ресурса <https://nav.sut.ru>) и сделать калибровку согласно инструкции программного обеспечения.
  - Разработать маршрут инспектирования.



- Провести инспектирование согласно маршруту.
- 3. Провести аналогичные измерения в домашней обстановке.
- 4. Представить лог-файл и тепловую карту с результатами инспектирования:
  - по уровню сигнала
  - по интерференции

### Методические указания.

При проведении инспектирования необходимо учитывать, что точность калибровки крайне важна для точности экспертизы. Обратите внимание, что необходимо выбрать частотный диапазон. Также на время инспектирования будет отключена возможность взаимодействия с другими устройствами по сети Wi-Fi.

При инспектировании старайтесь минимизировать колебания измерительного комплекса. Идеальным вариантом является использование специальных тележек.

Инспектирование проводится один раз. В лог-файлах записывается информация об уровне сигнала, интерференции, типе и местоположении точек доступа. Например, в ПО TamoGraph Site Survey (рис. 1) после инспектирования необходимо выбрать вкладку «Визуализация», в которой выбрать необходимый параметр. Слева в пункте меню можно видеть список точек доступа с необходимыми параметрами (SSID, стандарт, производитель). Также на тепловой карте указаны точки местонахождения точек доступа. Отметим, что локализация местонахождения точек доступа может происходить с существенной погрешностью.

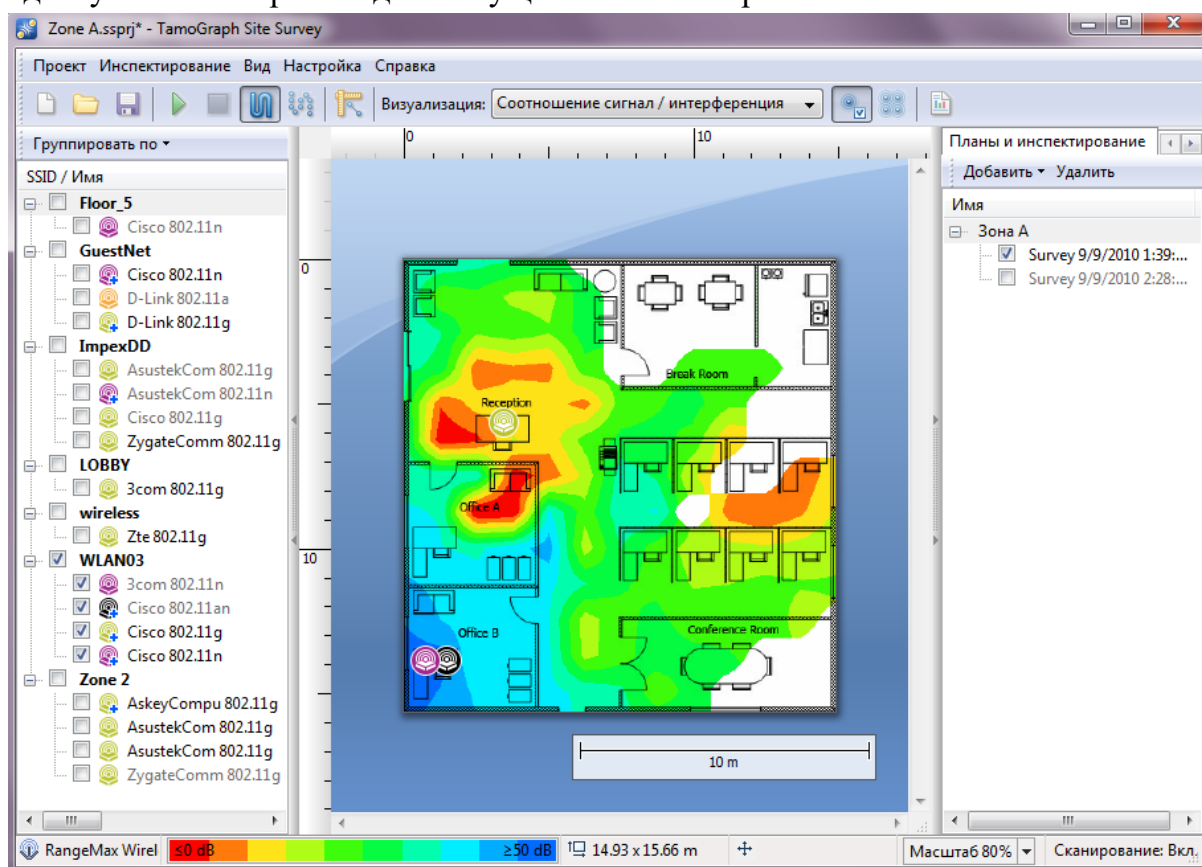


Рисунок 1 – Пример работы TamoGraph Site Survey (источник: [www.tamos.ru](http://www.tamos.ru))



При работе с пробной версией Acrylic Wi-Fi Heatmaps функционал почти полностью сохранен, есть также возможность построения тепловой карты в 3D. При этом поддерживается возможность генерации расширенного отчета (рис.2).

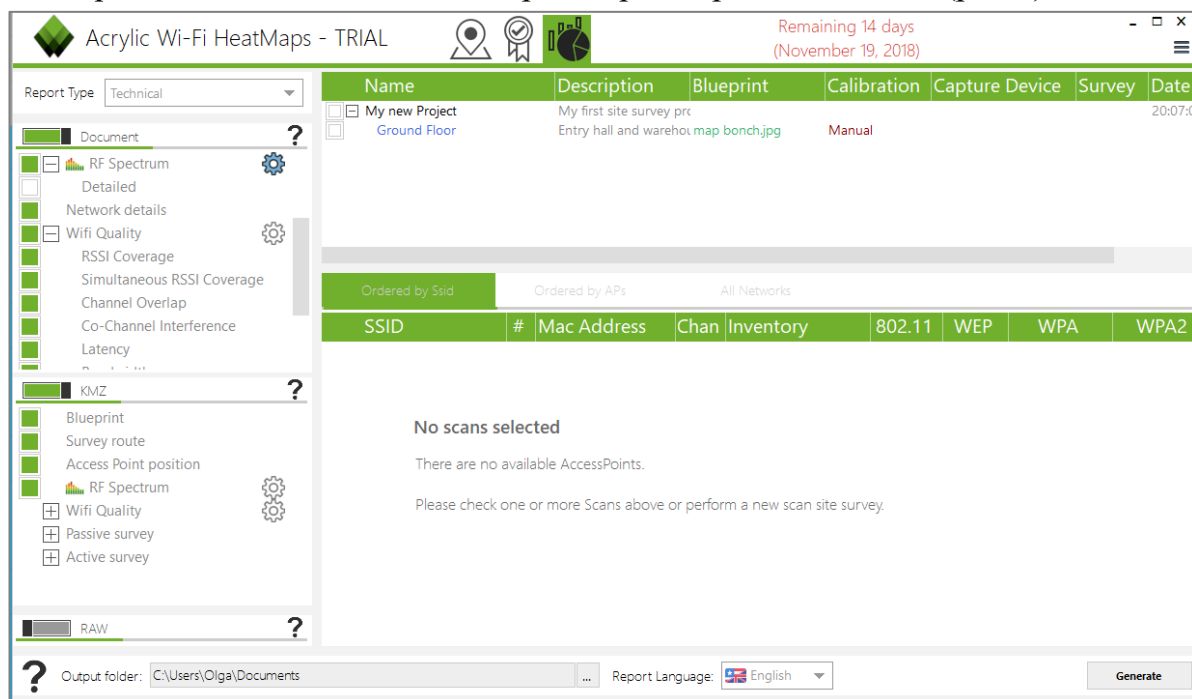


Рисунок 2 – Окно отчетов Acrylic Wi-Fi Heatmaps

**К защите:** подготовить отчет, в котором представить разработанный маршрут измерений, тепловую карту измерения уровня сигнала и интерференции по всем объектам, обработанные результаты измерений и анализ ситуации, указать на карте источники электромагнитного воздействия.

#### 4. Исследование показателей качества технологии Wi-Fi

**Цель работы:** исследовать характеристики качества обслуживания в сети Wi-Fi

**Задание:**

Важно: лабораторная работа проводится с использованием беспроводных маршрутизаторов, поэтому в процессе проведения работы результаты могут отличаться в зависимости от модели оборудования.

1. Собрать установку согласно рисунку 1. В качестве анализатора трафика рекомендуется использовать WireShark.

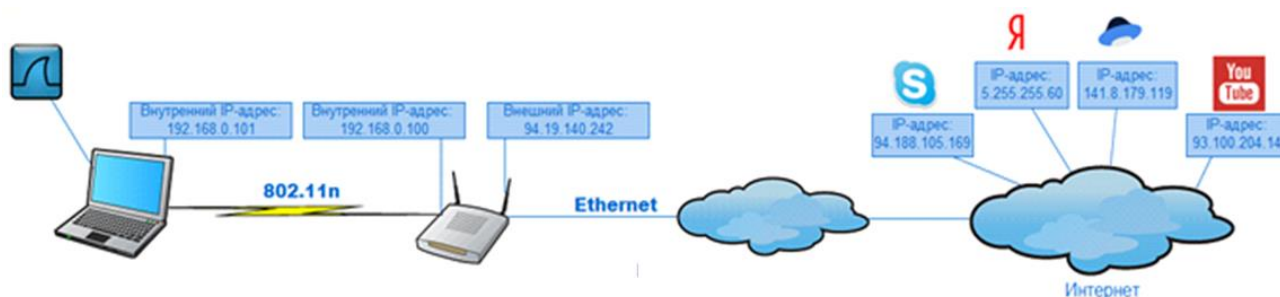


Рисунок 1 – Схема лабораторного макета

2. Создать потоки данных различных типов: голосовой трафик, видеотрафик, вебсерфинг и загрузка. Для генерации мультимедийных сервисов можно воспользоваться источниками в сети Интернет.
3. Выполнить анализ статистики по каждому из потоков с использованием режима WMM и в его отсутствие по временам прихода пакетов.
4. Построить соответствующие гистограммы распределения, используя табличный редактор, и провести сравнительный анализ.

### Методические указания

Для грамотной установки фильтров в анализаторе Wireshark с помощью командной строки (рис 2) определите IP-адрес компьютера, физический адрес сетевого адаптера, а также адрес основного шлюза, для внесения необходимых настроек в параметры организации сети. Для этого в окне командной строки введите команду `ipconfig /all`.

```

Адаптер беспроводной локальной сети Беспроводная сеть:

DNS-суффикс подключения . . . . . : 
Описание . . . . . : [CommView] Atheros AR9485WB-EG Wireless Network Adapter
Физический адрес . . . . . : 24-8A-64-AD-02-EF
DHCP-включен . . . . . : Да
Автонастройка включена . . . . . : Да
Локальный IPv6-адрес канала . . . . : fe80::7cb0:c438:7a6e:9137%17(Основной)
IPv4-адрес . . . . . : 192.168.0.101(Основной)
Маска подсети . . . . . : 255.255.255.0
Аренда получена . . . . . : 31 мая 2018 г. 20:04:11
Срок аренды истекает . . . . . : 1 июня 2018 г. 0:54:32
Основной шлюз . . . . . : 192.168.0.1
DHCP-сервер . . . . . : 192.168.0.1
IAID DHCPv6 . . . . . : 86248036
DUID клиента DHCPv6 . . . . . : 00-01-00-01-21-6D-8C-14-10-FE-ED-29-54-9D
DNS-серверы . . . . . : 192.168.0.1
NetBios через TCP/IP . . . . . : Включен
  
```

Рис.2. Определение ip-адресов для организации сети

В качестве исходных данных использовать компьютер, для этого сохраним в настройках маршрутизатора (рис 3) соответствующие изменения.

**TP-LINK®** Беспроводной Маршрутизатор серии N, до 150Мбит/с  
Модель № TL-WR740N/TL-WR740ND

**Настройки беспроводного режима**

Имя сети:  (Также называется SSID)

Регион:

Предупреждение: Убедитесь, что вы правильно выбрали страну, чтобы соответствовать местным законам. Некорректные настройки могут вызвать помехи.

Канал:

Режим:

Ширина канала:

☒ Включить беспроводное вещание роутера

☒ Включить широкоевещание SSID

☐ Включить WDS

**Справка: Настройки беспроводного режима**

**Примечание:** Дальность передачи данных или зона покрытия вашего беспроводного соединения в значительной степени зависят от физического расположения маршрутизатора. Для наилучшего результата размещайте ваш маршрутизатор:

- Рядом с предполагаемым центром зоны, в которой вы планируете использовать вашу беспроводную станцию.
- Над рабочей зоной на высоте, например, на шкафу.
- Вдали от потенциальных источников интерференции, таких как компьютеры, микроволновые печи и проводные телефоны.
- С вертикально поднятой антенной.
- Вдали от больших металлических поверхностей.

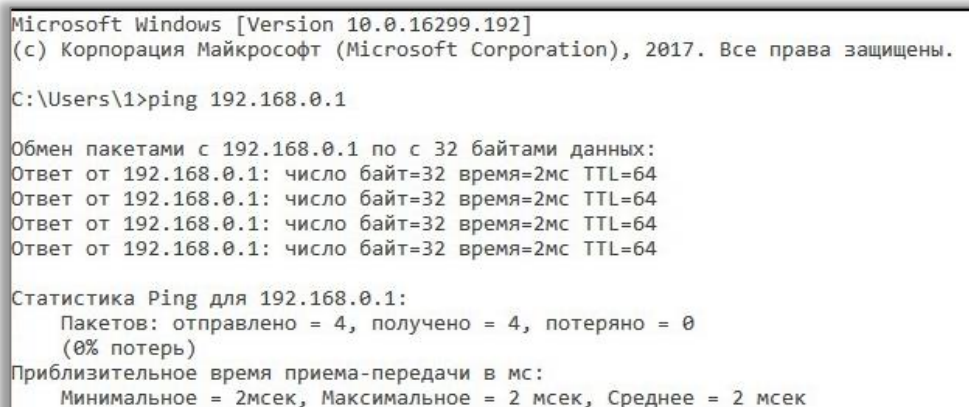
**Внимание:** Несоблюдение настоящих инструкций может привести к значительному снижению производительности вплоть до невозможности подключиться в беспроводном режиме к вашему маршрутизатору.

**Имя сети** - Введите имя длиной до 32 символов. Аналогичное имя (SSID) должно быть присвоено всем беспроводным устройствам в вашей сети.

Рис.3. Пример конфигурации маршрутизатора

Для проверки сетевого подключения между компьютером и маршрутизатором нужно в командной строке `cmd` ввести команду `ping 192.168.0.1` (рис. 4). Исследование

необходимо проводить в двух режимах: без использования функции WMM и с использованием WMM. Для этого в окне настроек маршрутизатора. Обычно это функция находится во вкладке «Расширенные настройки».



```
Microsoft Windows [Version 10.0.16299.192]
(c) Корпорация Майкрософт (Microsoft Corporation), 2017. Все права защищены.

C:\Users\1>ping 192.168.0.1

Обмен пакетами с 192.168.0.1 по 32 байтами данных:
Ответ от 192.168.0.1: число байт=32 время=2мс TTL=64
Ответ от 192.168.0.1: число байт=32 время=2мс TTL=64
Ответ от 192.168.0.1: число байт=32 время=2мс TTL=64
Ответ от 192.168.0.1: число байт=32 время=2мс TTL=64

Статистика Ping для 192.168.0.1:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
Приблизительное время приема-передачи в мс:
    Минимальное = 2мсек, Максимальное = 2 мсек, Среднее = 2 мсек
```

Рис.4. Проверка сетевого подключения

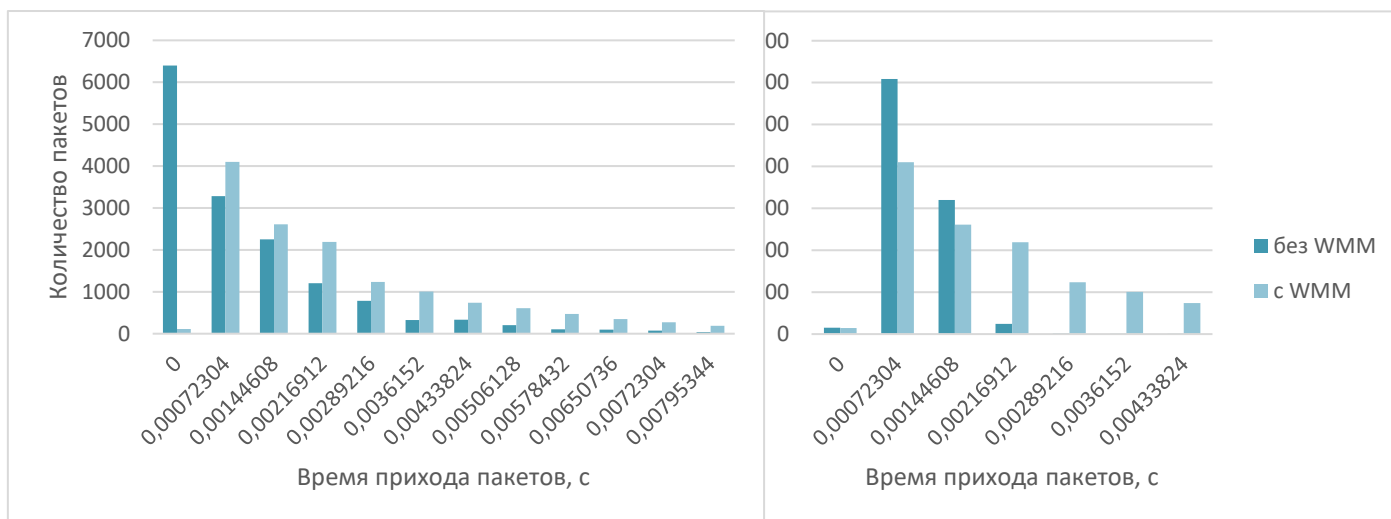
Исследование необходимо проводить в двух режимах: без использования функции WMM и с использованием WMM. Для этого в окне настроек маршрутизатора. Обычно это функция находится во вкладке «Расширенные настройки».

Для сбора статистики используем WireShark. Его необходимо запустить до начала генерации трафика. Для генерации трафика используйте ресурсы, указанные преподавателем.

Будем генерировать трафик в течение 5 минут, после чего дампы сохраняем в формате pcapng. Чтобы проанализировать каждый тип трафика отдельно, необходимо провести фильтрацию по одному потоку: для входящего трафика выставить фильтр `ip.src==<ip_addr>`, для исходящего: `ip.dst==<ip_addr>`.

Назначим необходимую фильтрацию по исходящему IP-адресу и, используя пункт меню *View → Time Display Format → Since Previous Captured Packet*, определим интервалы между поступлениями пакетов. Выбрав в меню *Edit* пункт *Set/Unset Time Reference* установим временную ссылку для текущего выбранного пакета. Аналогичную работу проделаем с остальными видами трафика, задавая соответственные параметры фильтрации.

Используя табличный редактор обработаем лог-файл WireShark и построим графики зависимости количества пришедших пакетов от времени для каждого из сервисов с использованием и без WMM (рис. 5). Легко видеть, что несмотря на то, что WMM увеличивает задержку потокового трафика (особенно видео), она позволяет уменьшить потери пакетов за счет уменьшения джиттера. Однако при этом задержка трафика данных может быть существенно увеличена



а) б)  
Рис. 5. Зависимость количества пакетов L2 от времени прихода с использованием и без функции WMM для: а) голосового трафика; б) видеотрафика

**К защите:** отчет должен содержать схему лабораторного стенда с указанием технических характеристик используемого оборудования, типы мультисервисного трафика и ресурсы генерации, результаты обработки лог-файлов, анализ и выводы о влиянии функции WMM на показатели качества обслуживания (задержку, джиттер задержки) в сети Wi-Fi.