**2 Материалы и методы исследования трафика корпоративной мультисервисной сети**

**2.1 Сбор сведений о корпоративной мультисервисной сети**

Для анализа трафика корпоративной мультисервисной сети рассмотрена реальная корпоративная сеть предприятия ГКУ «Управление Сахалинавтодор». Предприятие «Управление Сахалинавтодор» осуществляет проектирование и строительство автомобильных дорог, содержанием автомобильных дорог.

Штат предприятия составляет 180 человек. Офисы предприятия располагаются в трех административных зданиях, которые располагаются на расстоянии трех километров друг от друга.

Корпоративная мультисервисная сеть предприятия строится на базе технологии SHDSL и состоит из:

* 170 рабочих станций пользователей;
* Структурированную кабельную систему на основе кабеля витая пара;
* Десять коммутаторов второго уровня модели OSI;
* Один маршрутизатор;
* Четыре сервера (сервер баз данных, сервер электронной почты, файловый сервер, сервер IP-телефонии);
* Оборудование видеонаблюдения.

Связь между офисами организуется при помощи ADSL-модемов, осуществляющих доступ в сеть Интернет. Для повышения безопасности информации используется услуга VPN-сервиса на стороне провайдера.

Структура мультисервисной сети организации и схематичное расположение сетевых элементов на плане здания представлено на рисунках 2.1-2.3.

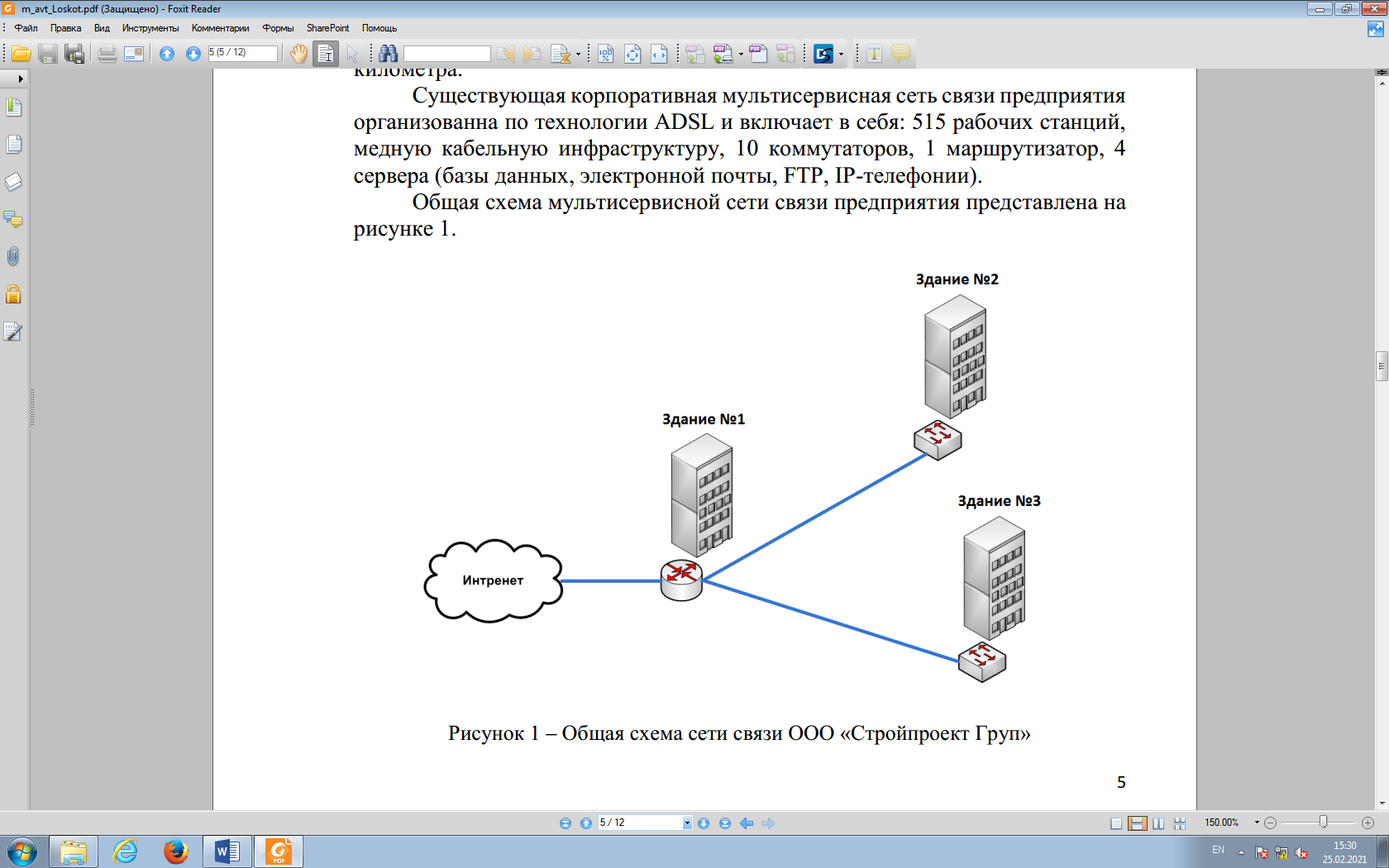


Рисунок 2.1 – Обобщенная схема сети ГКУ «Управление Сахалинавтодор»

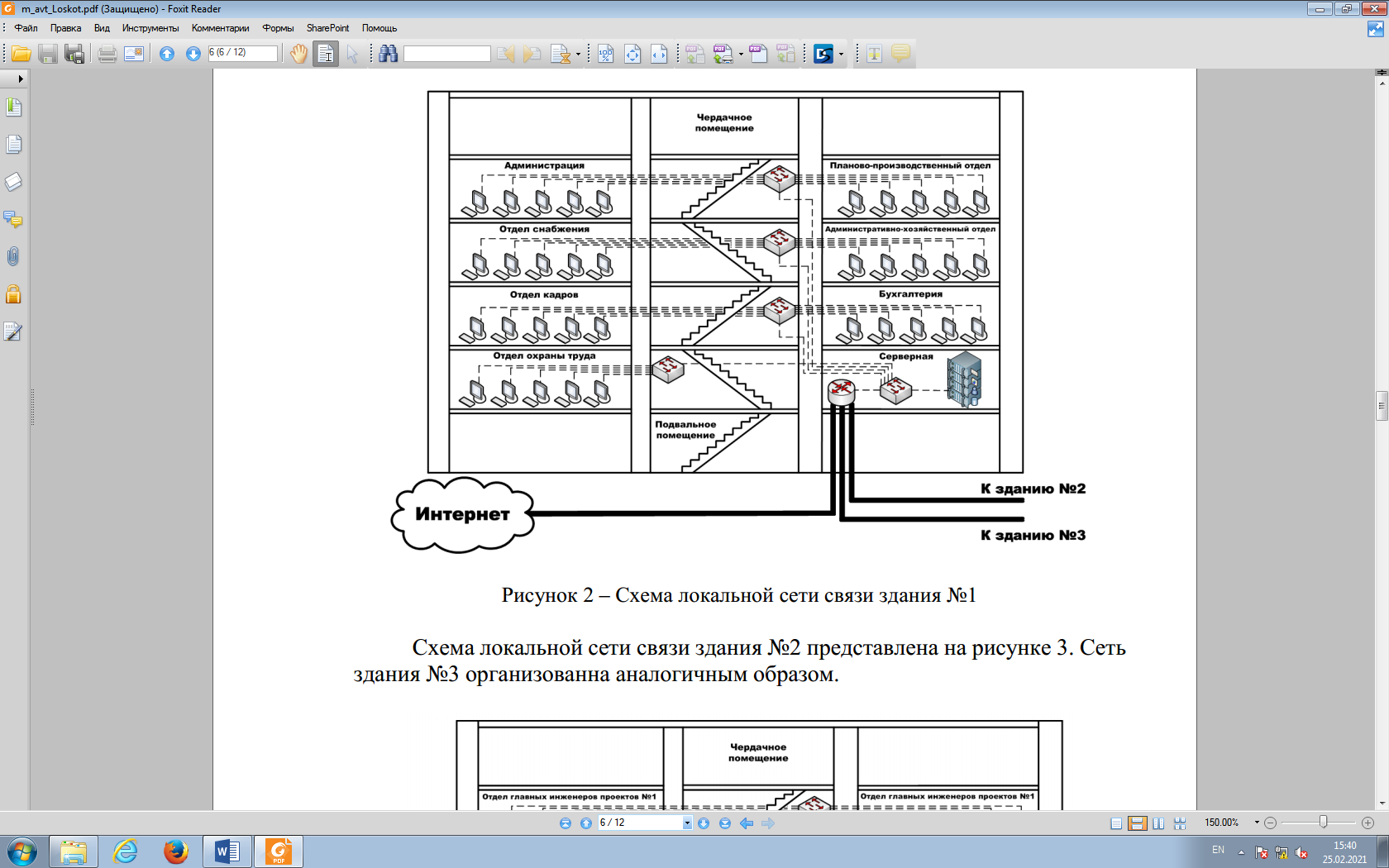


Рисунок 2.2 – Схема сети здания №1

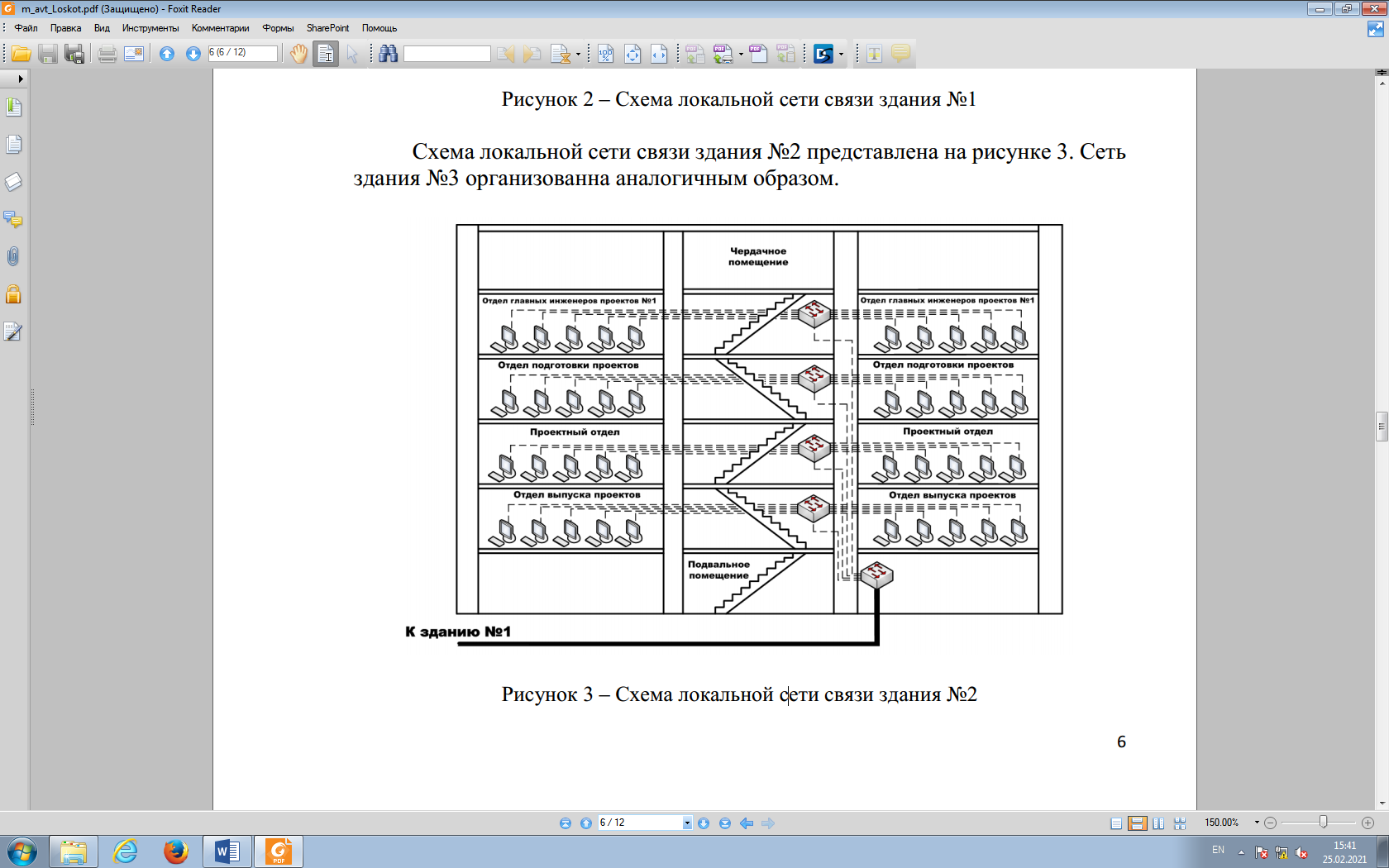


Рисунок 2.3 – Схема сети здания №2

Схема сети здания №3 аналогична схеме сети здания №2.

Анализ структуры сети предприятия показал, что используемая сетевая инфраструктура не способна удовлетворить возрастающие потребности пользователей. Используемое на предприятии каналообразующие оборудование (ADSL-модемы) не может увеличить пропускную способность на данных расстояниях и используемых типах кабелей. Перегрузки коммутационного и серверного оборудования повышают частоту выхода из строя данного оборудования и, как следствие, расходы предприятия.

Также участились жалобы пользователей на низкую скорость доступа в сеть, большое время отклика ресурсов (баз данных, электронной почты, сервиса IP-телефонии) корпоративной мультисервисной сети.

Здесь стоит привести требования к надежности корпоративной сети и некоторую статистику по показателям качества в существующей сети (задержкам, потерям, скорости передачи, алармам и отказам), чтобы обосновать переход на более надежные системы, среды, топологии.

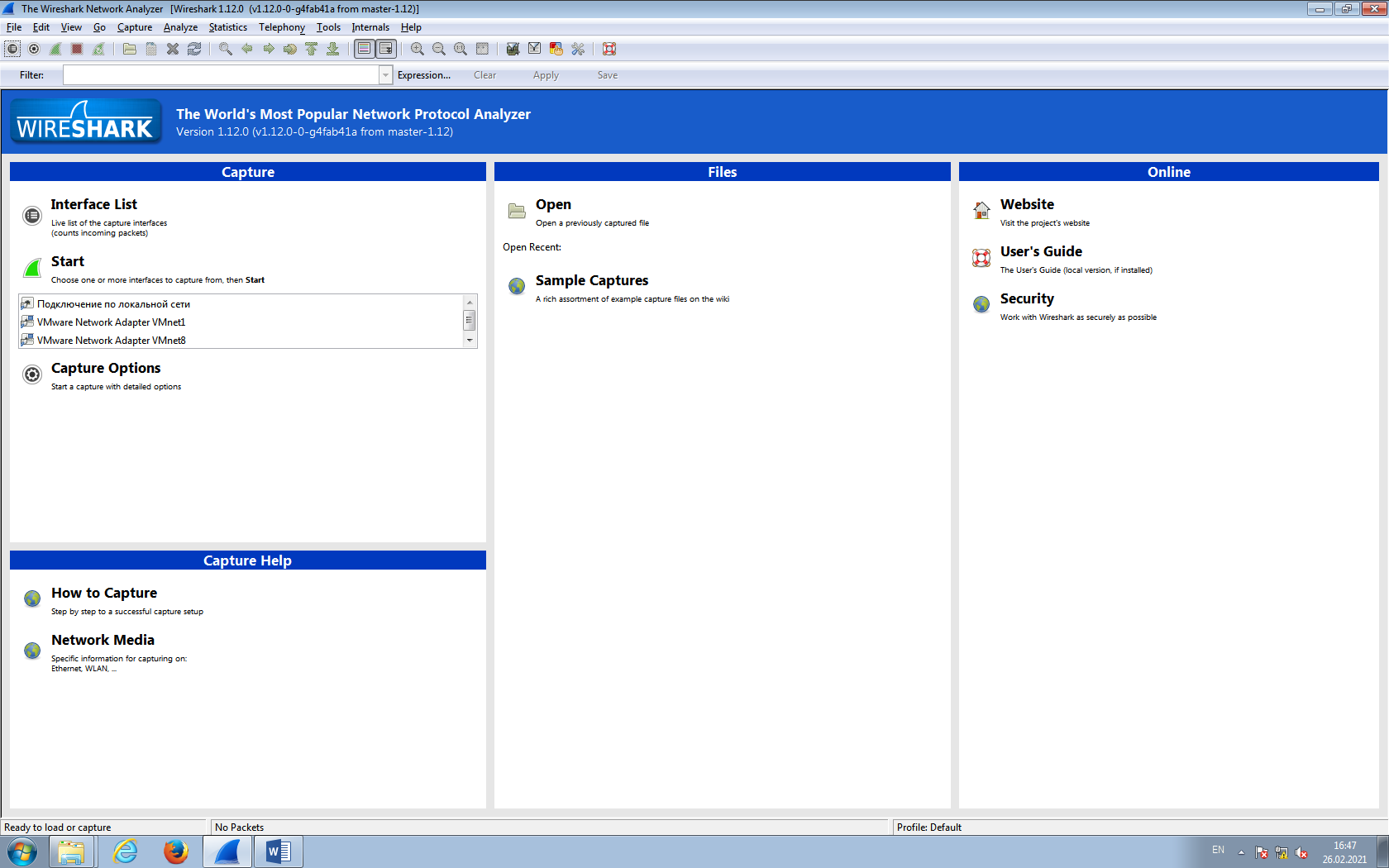
Анализ структуры телекоммуникационной сети позволил предъявить к ней следующий набор требований:

* Обеспечение отказоустойчивости сети и ее отдельных элементов;
* Обеспечение надежности сети предприятия;
* Обеспечение требуемой производительности сети;
* Обеспечение масштабируемости сети и гибкости ее составных элементов;
* Обеспечение требуемого уровня информационной безопасности сети;
* Повышение пропускной способности ядра сети;
* Модернизация структурированной кабельной системы;
* Обновление коммутационного и серверного оборудования, включая программное обеспечение.

**2.2 Средства и инструменты исследования трафика**

Для решения задач оценки интенсивности трафика в исследуемой сети, а также для оценки основных характеристик качества обслуживания пользователей: задержки передачи пакетов, времени отклика на запросы пользователя и других характеристик использован анализатор трафика Wireshark.

После запуска сетевого анализатора Wireshark главное окно программы имеет вид, представленный на рисунке 2.4.



**1**

Рисунок 2.4 – Главное окно программы Wireshark

Для захвата пакетов в режиме реального времени необходимо выбрать сетевую карту, установленную на компьютере (элемент 1 на рисунке 2.4).

Для открытия уже сохраненного файла с информацией о принятых пакетах, необходимо перейти в раздел меню «Файл» и выбрать пункт «Открыть» (рисунок 2.5).

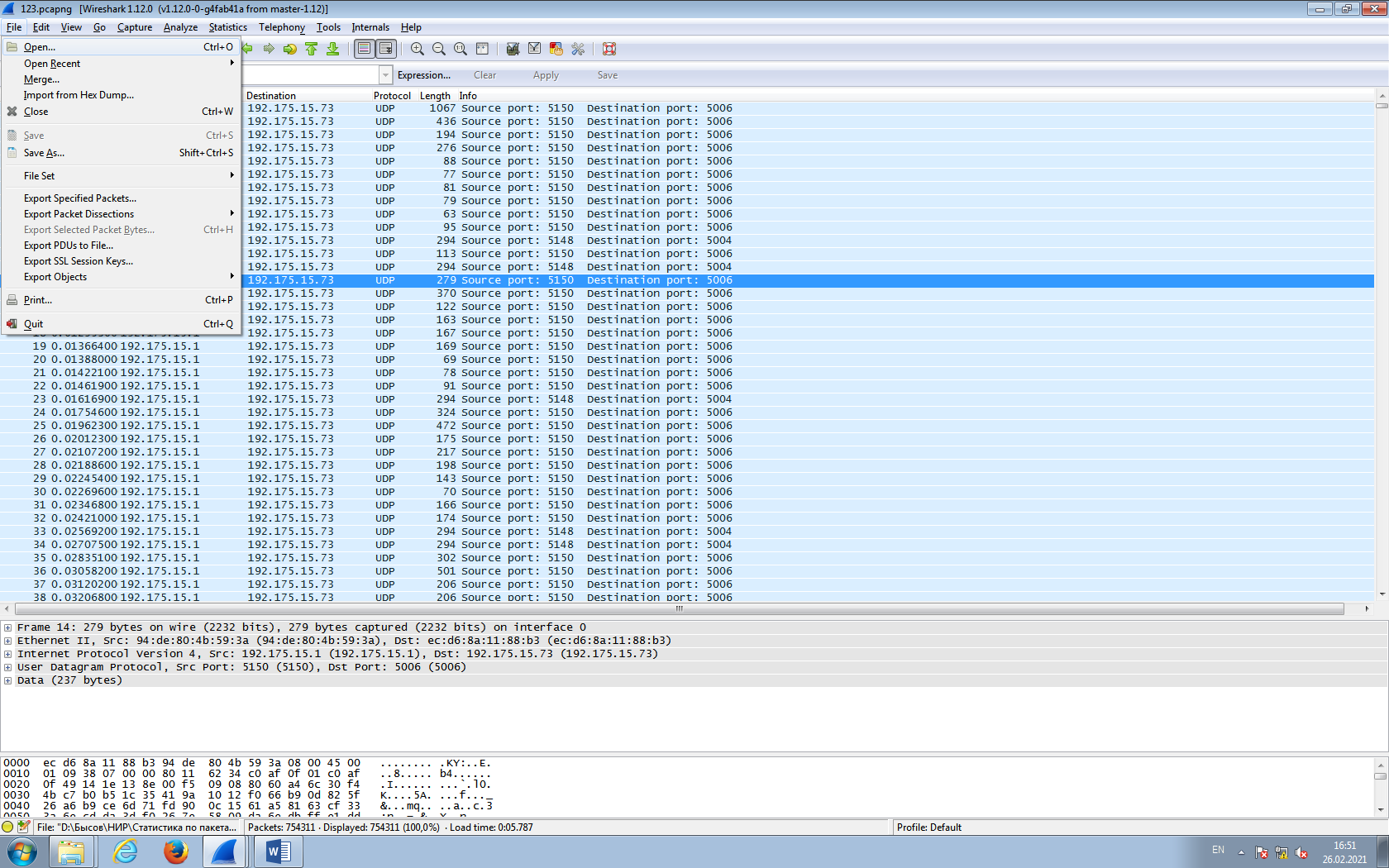
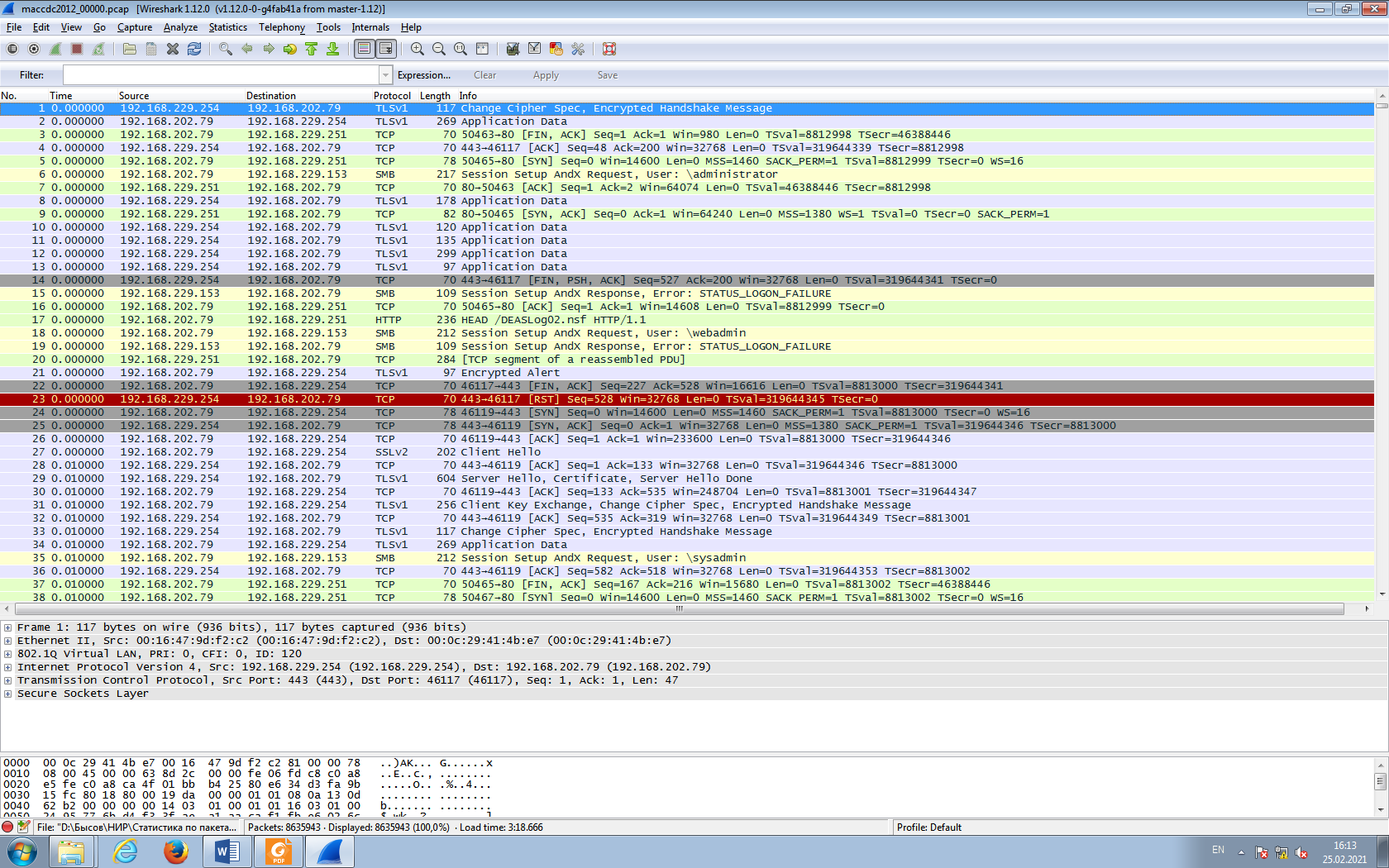


Рисунок 2.5 – Меню «Файл» главного окна программы Wireshark

После открытия файла окно программы примет вид, представленный на рисунке 2.6.

**1**



**4**

**3**

**2**

**1**

Рисунок 2.6 – Главное окно программы Wireshark окно программы с информацией о пакетах

Главное окно программы Wireshark включает панель меню и панель быстрого доступа элементы 1 и 2 соответственно на рисунке 2.6. Под панелью быстрого доступа находится панель для настройки фильтров (элемент 3 на рисунке 2.6). Под панелью фильтров находится панель с информацией о принятых пакетах (элемент 4 на рисунке 2.6). В таблице данной панели представлена следующая информация:

* Условный номер принятого пакета (№);
* Время регистрации пакета (Time);
* IP-адрес узла-источника (Source);
* IP-адрес узла назначения (Destination);
* Протокол (Protocol);
* Длина пакета (Length);
* Дополнительная информация о принятом пакете (Info).

Далее следует панель с детальной информацией по выделенному пакету (рисунок 2.7).

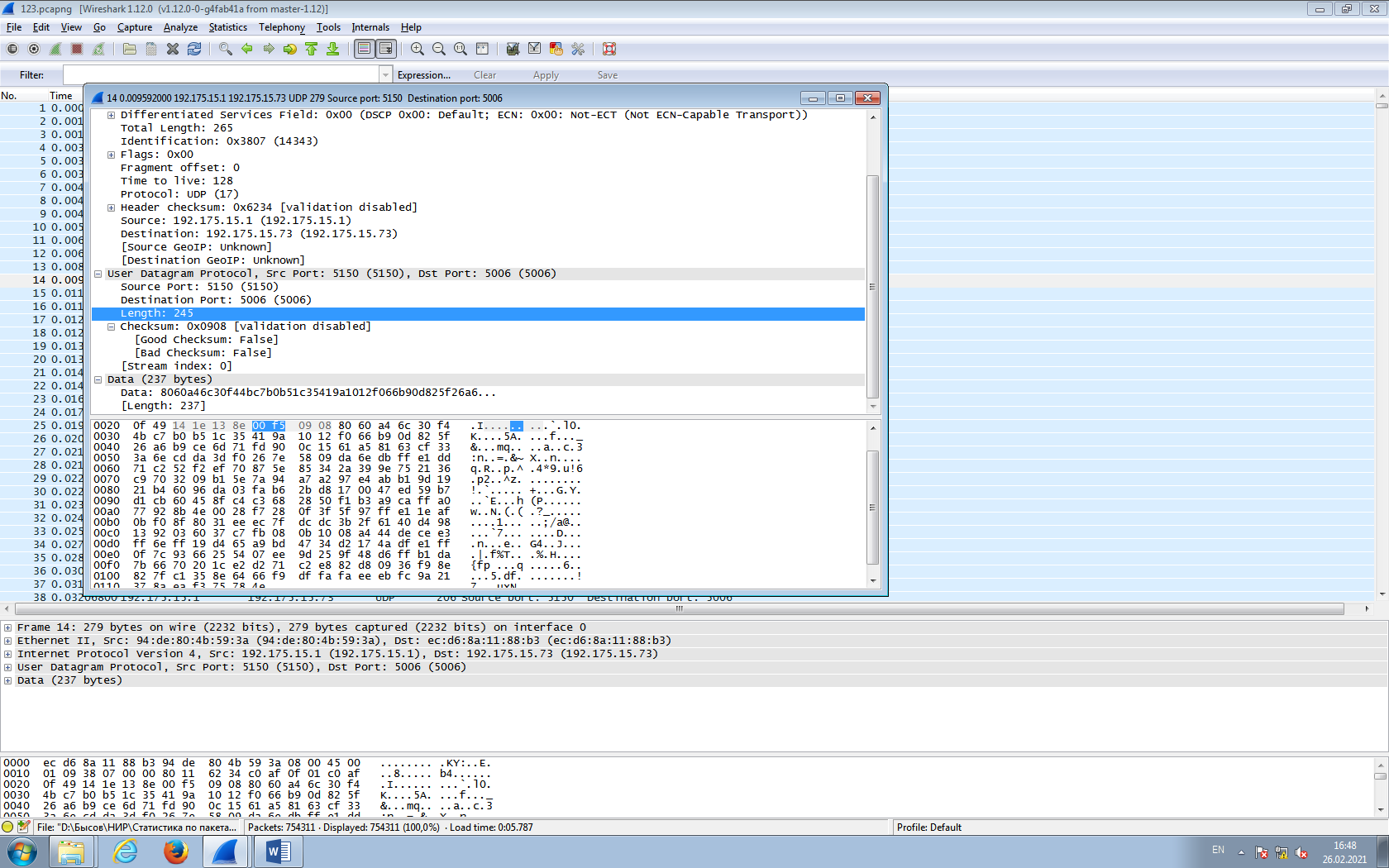


Рисунок 2.7 – Панель программы с детальной информацией о структуре пакета

В панели представлено содержимое пакета в соответствии с эталонной моделью взаимодействия открытых систем. Информация о пакетах представлена в виде дерева, ветви которого можно раскрывать для просмотра содержимого пакета на определенном уровне. Нижняя часть панели содержит дамп пакетов в шестнадцатеричной форме.

Панель «Меню» содержит пункты с интуитивно понятным назначением (рисунок 2.8).

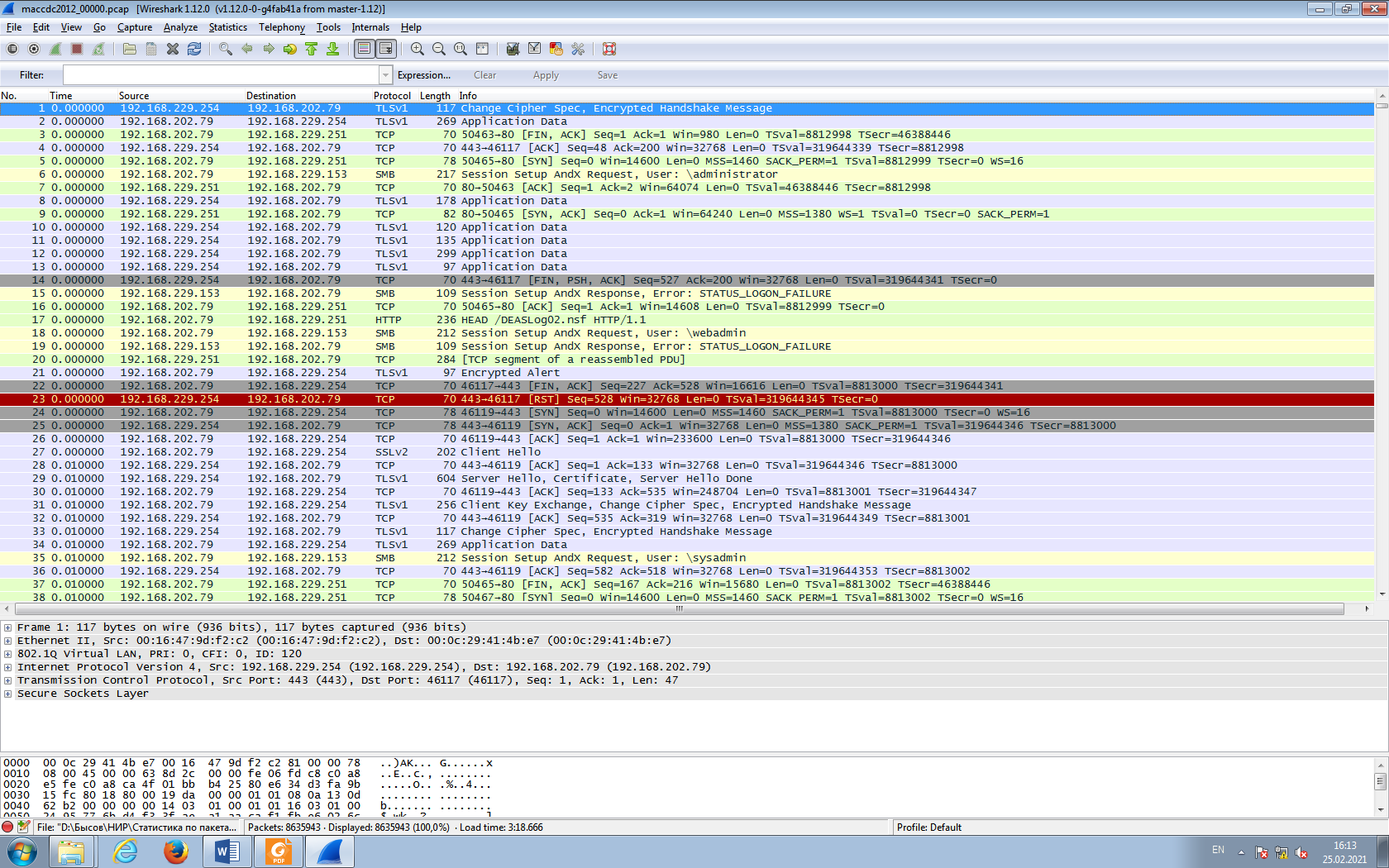
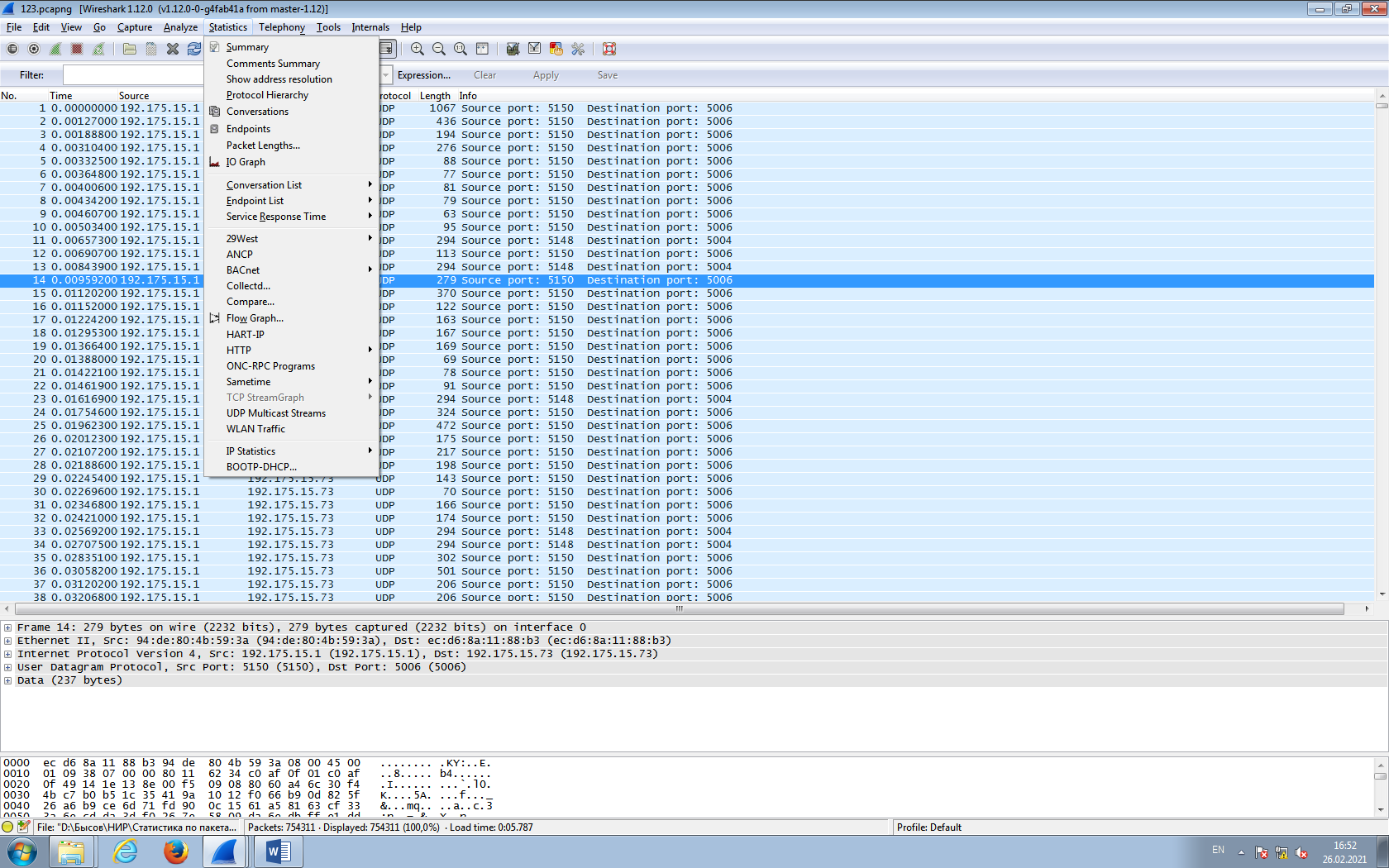


Рисунок 2.8 – Панель «Меню» и панель быстрого доступа

Для просмотра информации по пакетам используется пункт меню «Statistics» (рисунок 2.9).



**3**

**2**

**1**

Рисунок 2.9 – Содержание пункта меню «Statistics»

Первым используемым пунктом является пункт «Иерархия протоколов» (пункт 1 на рисунке 2.9). Обзор статистики в соответствии с данным пунктом представлено на рисунке 2.10.

Пункт «Иерархия протоколов» содержит информацию об абсолютном и процентном отношении принятых байт и пакетов определенного протокола, а также скорость следования пакетов данного протокола. Информация представляется таблично. Колонка «Протокол» имеет древовидную структуру с различной детализацией.

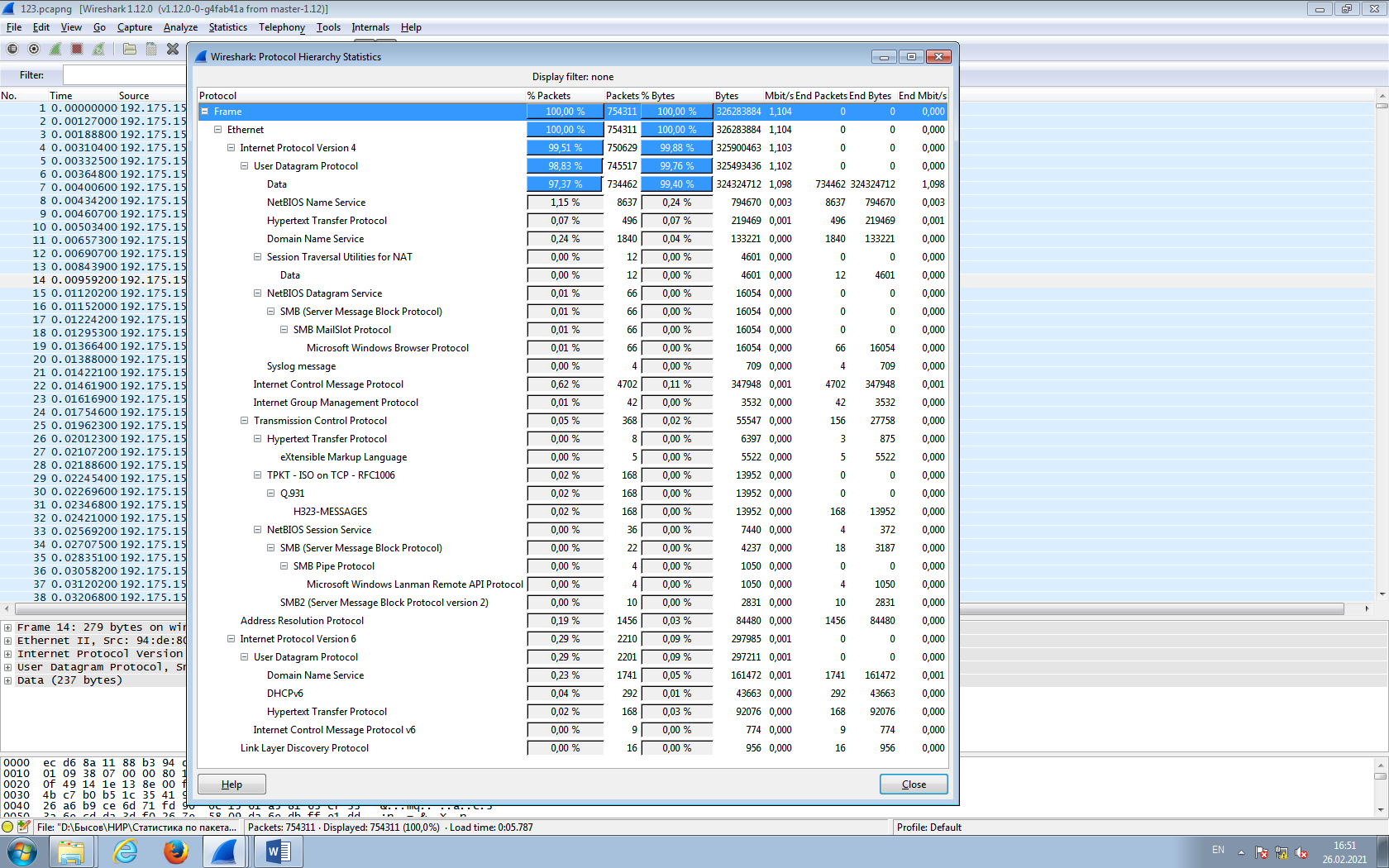


Рисунок 2.10 – Пример окна «Иерархия протоколов»

Следующим важным пунктом для обобщенного анализа длин принятых пакетов является пункт «Длина пакетов» (элемент 2 на рисунке 2.11). Пример окна «Длина пакетов» представлено на рисунке 2.11.

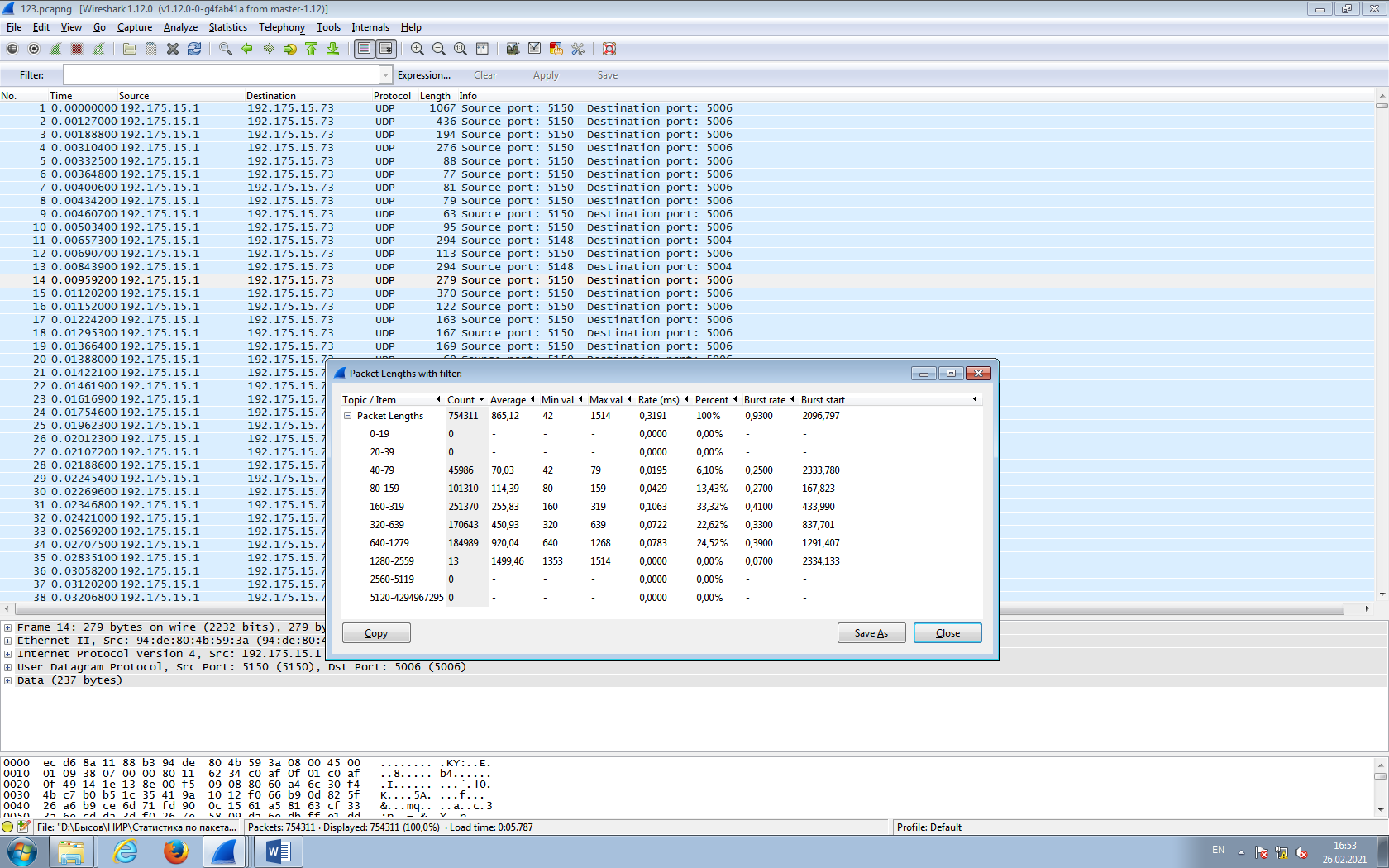


Рисунок 2.11 – Пример окна «Длина пакетов»

Для построения зависимости интенсивности мультисервисного трафика от времени используется пункт меню «График интенсивности» (элемент 3 на рисунке 2.9). Сетевой анализатор позволяет строить зависимости интенсивности трафика измеряемой как в бит/c (рисунок 2.12), так и ‑ пакет/с (рисунок 2.13).

Мультисервисный трафик имеет пульсирующий характер, причем амплитуда пульсаций имеет достаточно большое значение относительно среднего значения.

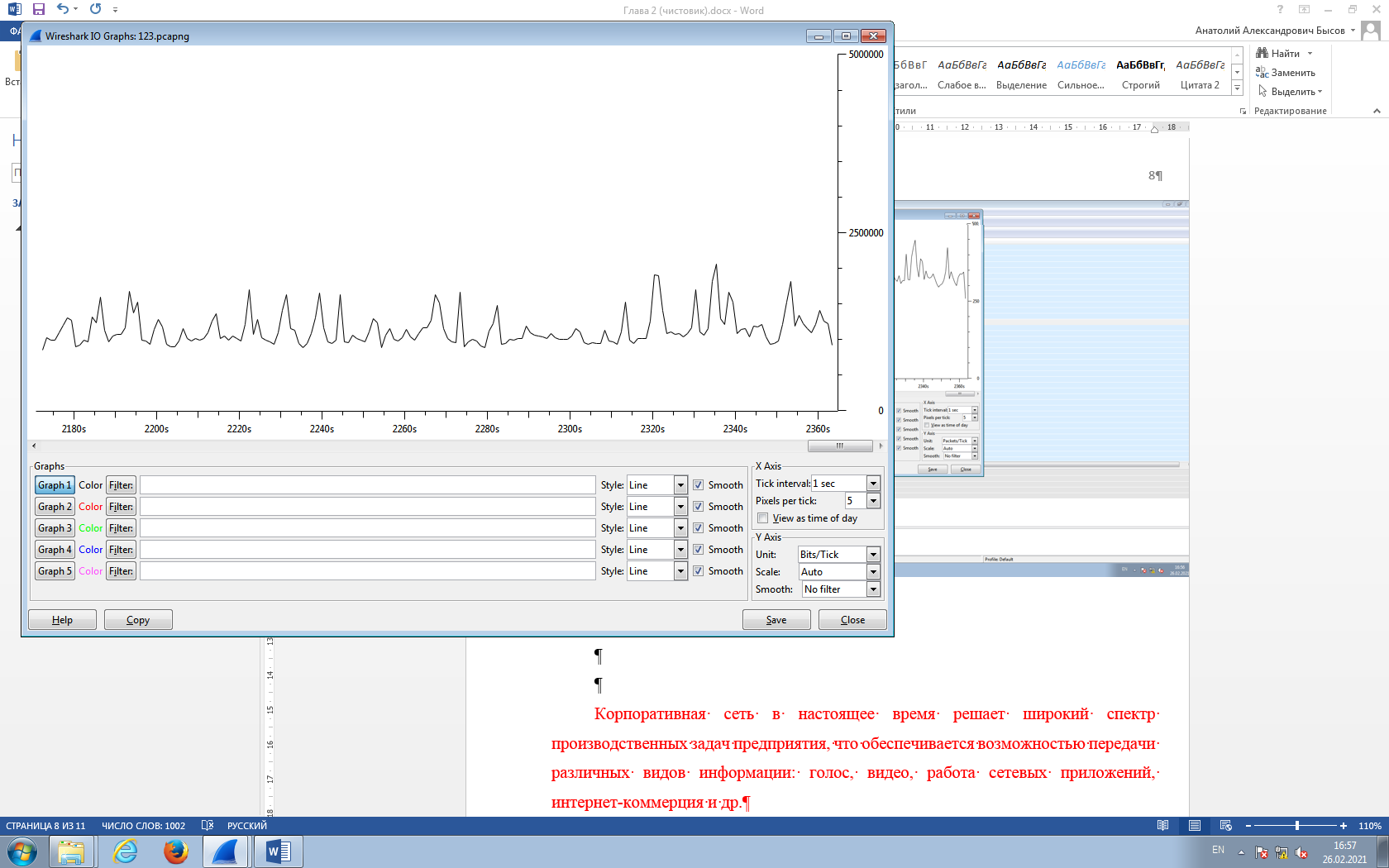


Рисунок 2.12 – Зависимость интенсивности мультисервисного трафика (бит/с) от времени

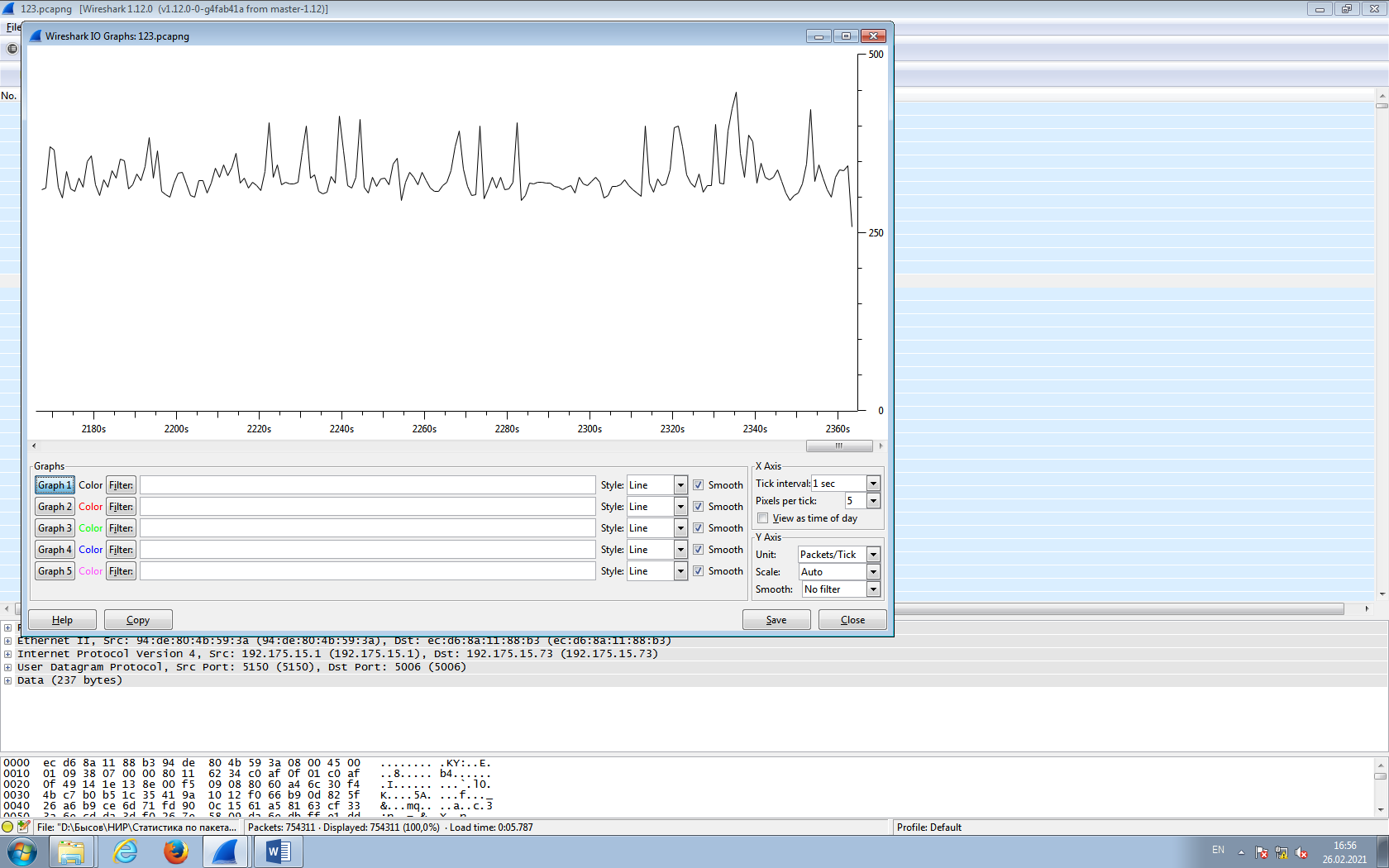


Рисунок 2.13 – Зависимость интенсивности мультисервисного трафика (пакет/с) от времени

Для исследования характеристик определенной группы пакетов используется панель «Фильтр» (рисунок 2.14).

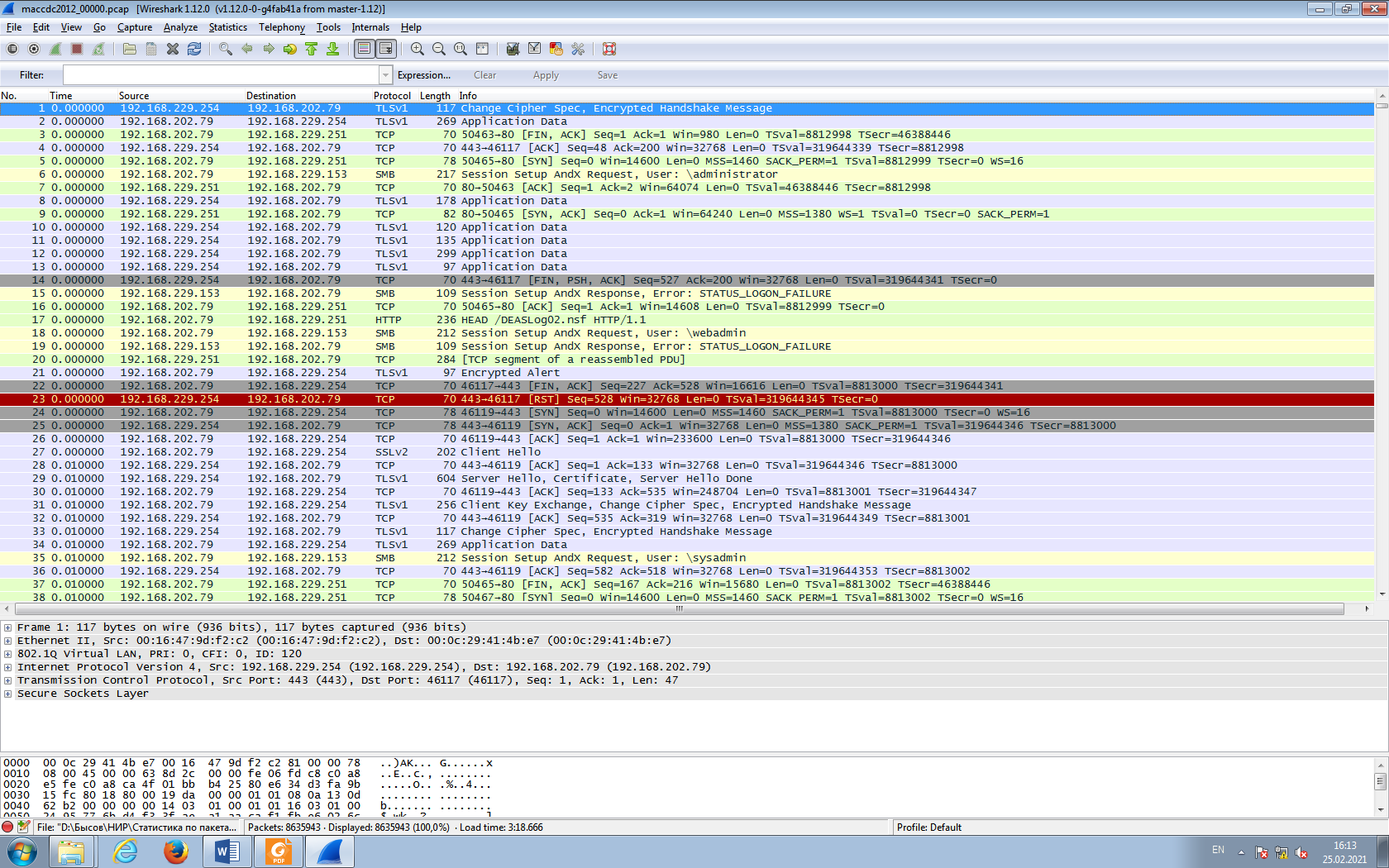


Рисунок 2.14 – Панель «Фильтр»

В программе можно как встроенные фильтры (рисунок 2.15), так и создавать пользовательские фильтры. Создание пользовательских фильтров основано на использовании операторов сравнения и логических операторов.

Основные операторы сравнения представлены в таблице 2.1.

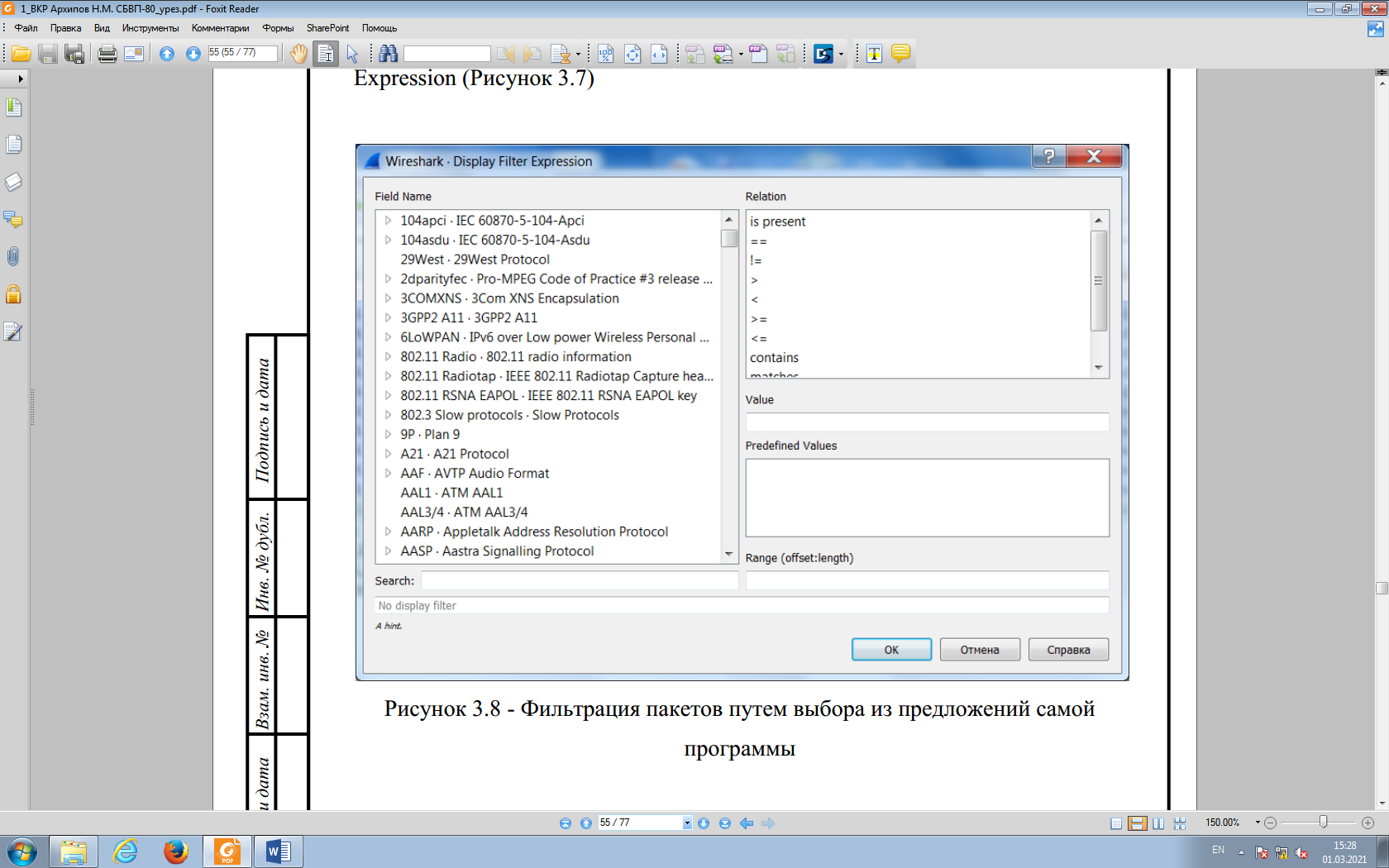


Рисунок 2.15 – Встроенные фильтры программы Wireshark

Таблица 2.1 – Основные операторы сравнения

|  |  |
| --- | --- |
| Оператор сравнения | Пояснение |
| tcp.ack | Подтверждения (ACK) протокола TCP |
| udp.port | Порт источника или получателя в сегменте протокола UDP |
| ip.proto | Обозначение протокола, который был инкапсулирован в пакет IP |
| tcp.srcport | Порт источника в сегменте протокола ТСР |
| tcp.dstport | Порт получателя в сегменте протокола ТСР |
| dns.resp.name | Имя сетевого ресурса в DNS ответе |
| dns.qry.name | Имя сетевого ресурса в DNS запросе |
| tcp.port | Порт источника или получателя в сегменте протокола ТСР |
| ip.addr | Сетевой адрес источника или получателя в пакете протокола IP |
| ip.src | Сетевой адрес источника в пакете протокола IP |
| ip.dst | Сетевой адрес получателя в пакете протокола IP |
| eth.addr | Физический адрес источника или получателя в кадре протокола Ethernet |
| eth.src | Физический адрес источника в кадре протокола Ethernet |
| eth.dst | Физический адрес получателя в кадре протокола Ethernet |
| eth.len | Длина кадра протокола Ethernet |

Для создания комбинированных фильтров используются логические операторы. Логические операторы и примеры их применения представлены в таблице 2.2.

Таблица 2.2 – Основные логические операторы

|  |  |  |
| --- | --- | --- |
| Логический оператор | Значение | Пример |
| > | больше | tcp.srcport>2000 ‑ отобразить только те сегменты протокола TCP, в которых порт источника больше 2000 |
| < | меньше | tcp.srcport<200 ‑ отобразить только те сегменты протокола TCP, в которых порт источника меньше 2000 |
| = = | равно | ip.addr==10.10.0.27 ‑ отображение пакетов с IP-адресом 10.10.0.27 источника или получателя |
| != | не равно | ip.dst!=255.255.255.255 ‑ не отображать широковещательные пакеты |
| && | логическое «и» | ip.src==10.10.0.27&&ip.dst10.10.0.30 ‑ отобразить только сообщения, отправленные устройством с IP-адресом 10.10.0.27 для устройства с IP-адресом 10.10.0.30. |

Таким образом, программа Wireshark имеет широкие возможности по исследованию мультисервисного трафика в корпоративных сетях. Для анализа трафика сетевой анализатор должен быть установлен на компьютер, который можно подключать в различных точках сети для регистрации трафика. Как правило анализаторы трафика устанавливаются в ядре мультисервисной сети для исследования агрегированных потоков трафика. Технически задача подключения регистрирующего компьютера решается путем перевода одного из интерфейсов коммутатора в режим «Зеркало» для параллельного захвата пакетов трафика без разрыва соединения.

**2.3 Анализ и классификация сетевого трафика**

В результате исследования трафика мультисервисной сети получены интенсивности трафика в ядре сети. Зависимость интенсивности трафика выраженной в бит/c и пакет/с представлены на рисунках 2.16 и 2.17 соответственно.

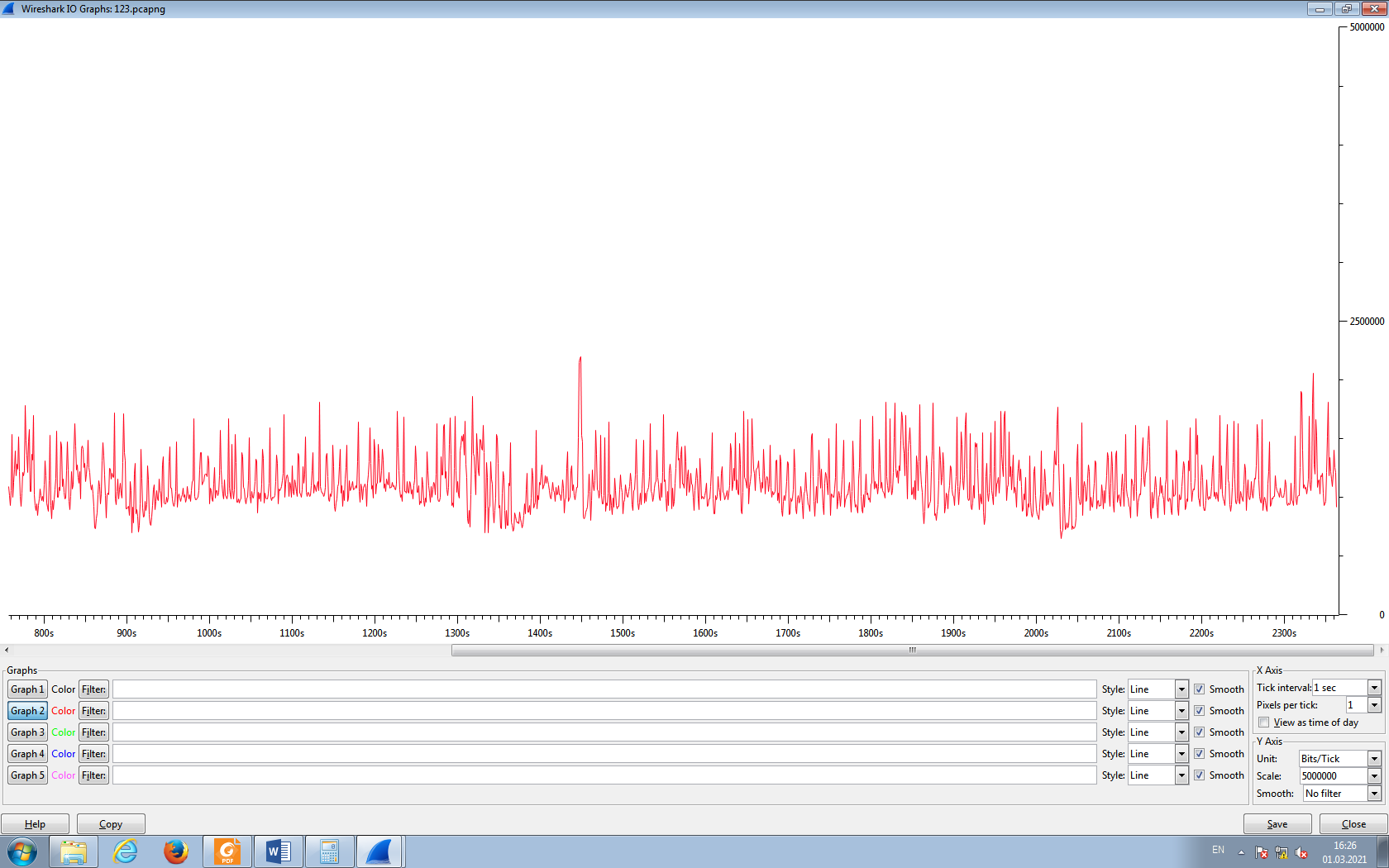


Рисунок 2.16 – Интенсивность мультисервисного трафика (бит/с)

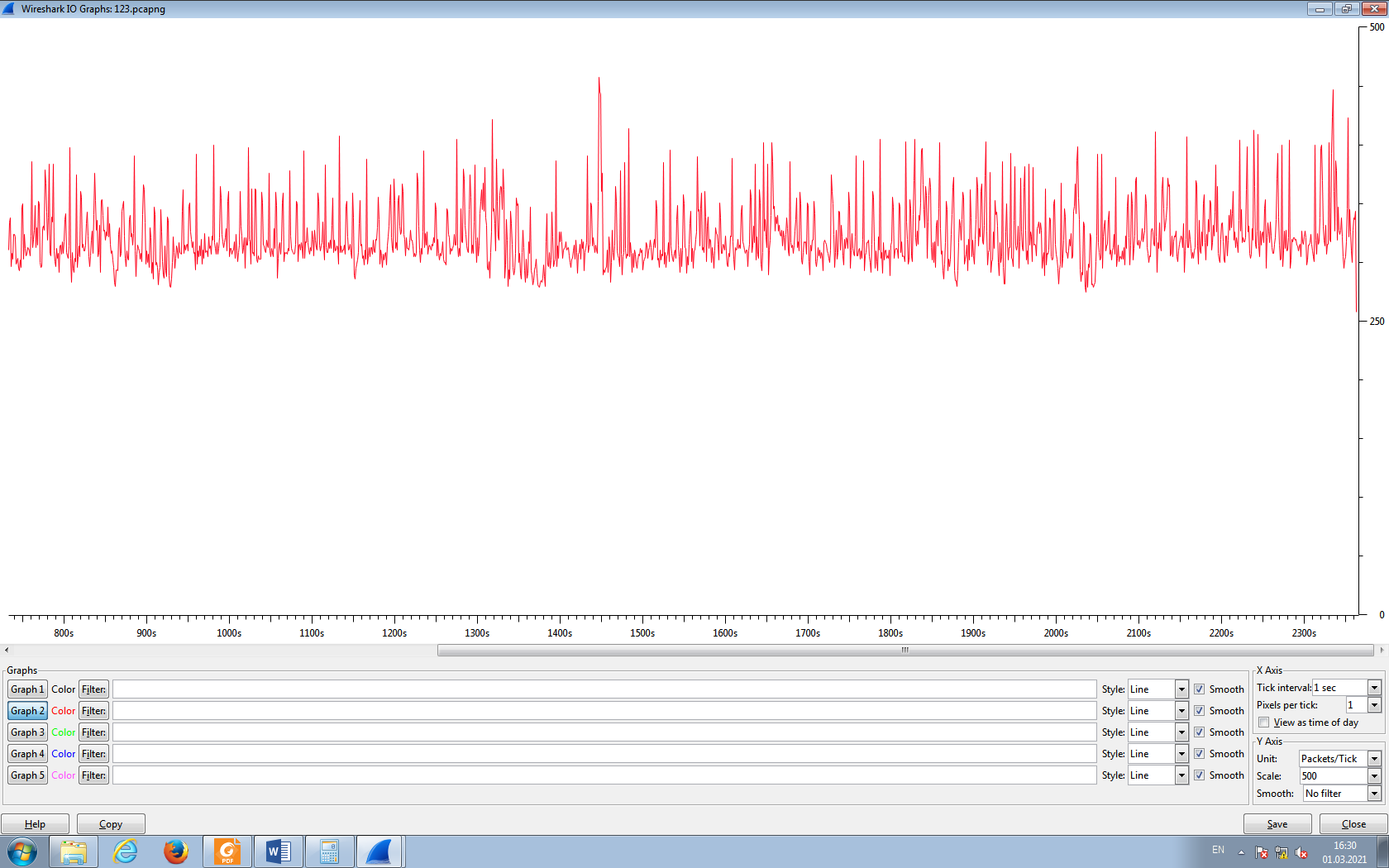


Рисунок 2.17 – Интенсивность мультисервисного трафика (пакет/с)

Для оценки среднего значения интенсивности мультисервисного трафика, проведено усреднение данных в программе. Среднее значение интенсивности, измеренное в бит/с и пакет/c представлено на рисунках 2.18 и 2.19 соответственно.

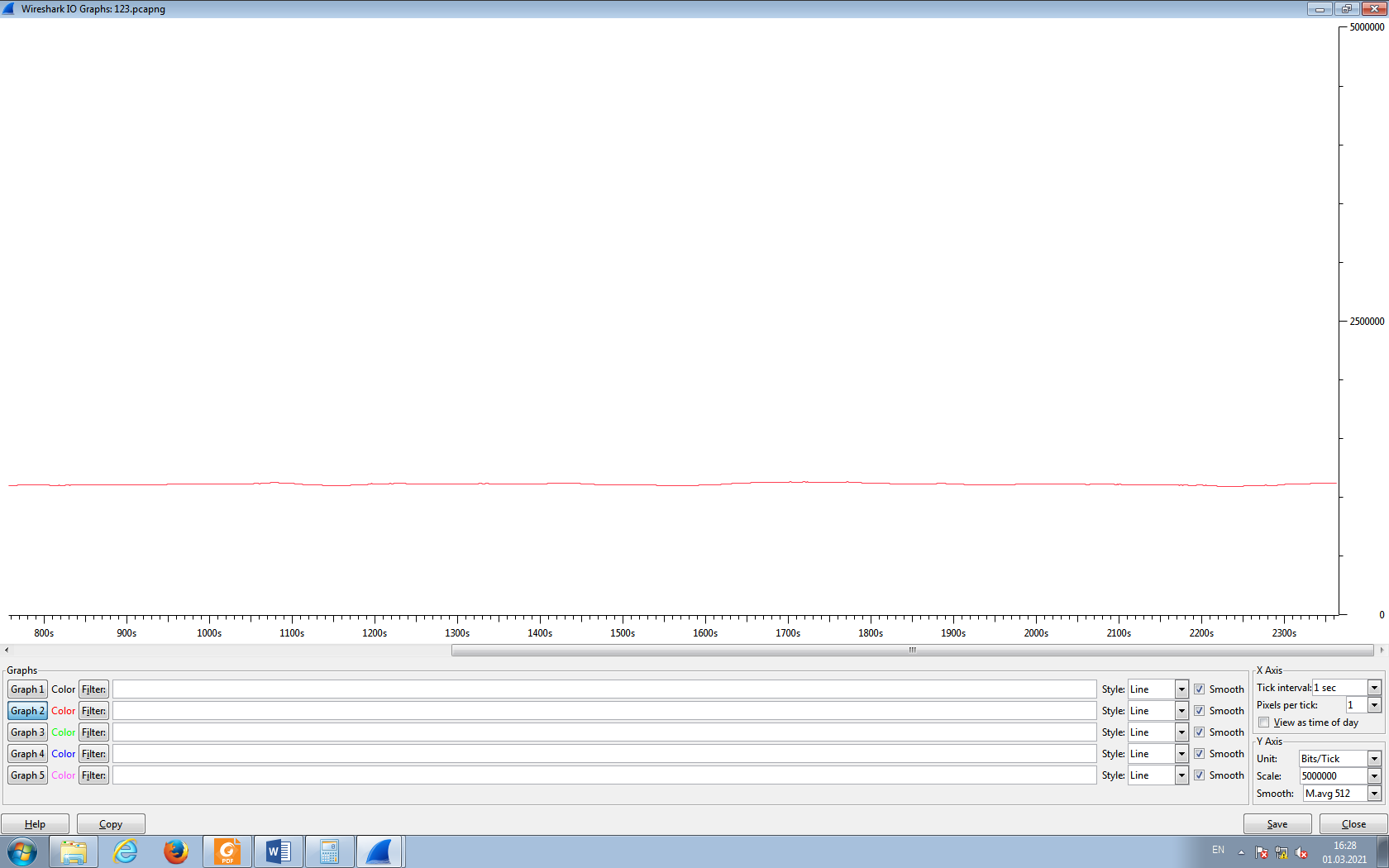


Рисунок 2.17 – Среднее значение интенсивности трафика (бит/с)

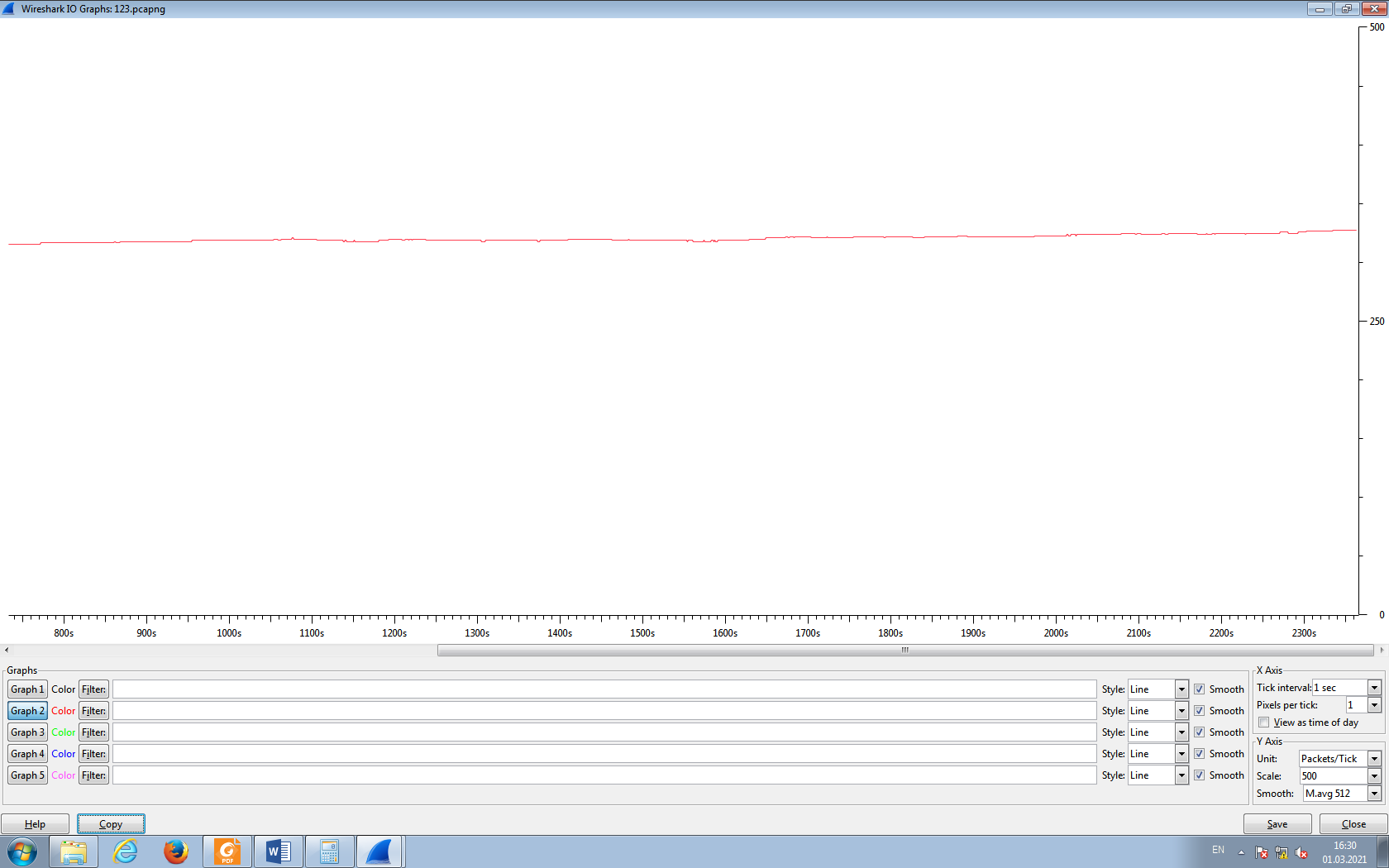


Рисунок 2.18 – Среднее значение интенсивности трафика (пакет/с)

На рисунках 2.15 и 2.16 показано, что из-за наличия входных и выходных буферов у коммутационных устройств пакеты следуют группами (пачками), что приводит к наличию пульсаций. Наблюдаемые пульсации имеют относительно невысокую длительность, однако, достаточно высокую амплитуду относительно среднего значения. Наличие пульсаций предполагает наличие существенного запаса по пропускной способности линий связи.

На рисунках 2.17 и 2.18 показано, что среднее значение интенсивности мультисервисного трафика составляет 1,2 Мбит/c или 330 пакетов/c.

Для дальнейшего анализа объемов трафика в зависимости от типа протокола транспортного уровня ЭМВОС. данные полученные в разделе «Иерархия протоколов» меню «Статистики» программы Wireshark перенесены в редактор Microsoft Office Excel. Структура мультисервисного трафика на транспортном уровне представлена на рисунке 2.19.

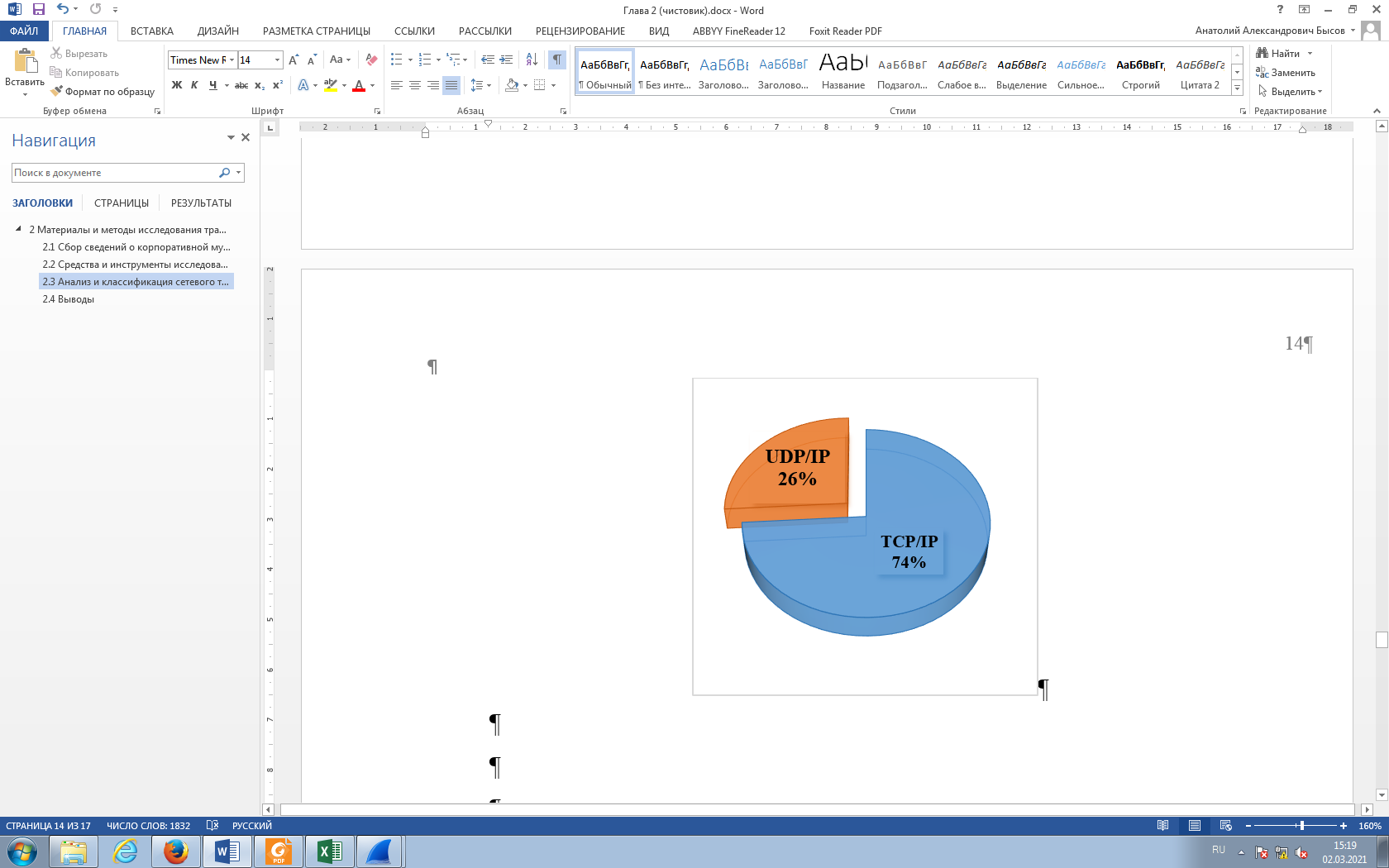


Рисунок 2.19 – Структура трафика на транспортном уровне

На рисунке 2.19 показано, что превалирующую часть пакетов на транспортном уровне передается в соответствии с протоколов гарантированной доставки пакетов (TCP). Однако существенную долю занимают пакеты, переданные в соответствии с протоколом транспортного уровня негарантированной доставки пакетов (UDP). Наличие 26% данных пакетов можно объяснить используемыми сервисами в сети, а именно системой видеонаблюдения (пакеты данного сервиса передаются, как правило, в соответствии с протоколом UDP для снижения средней задержки передачи пакетов).

Дальнейший анализ проведен в соответствии с используемыми приложениями внутри стеков TCP/IP и UDP/IP.

Распределение пакетов в соответствии со стеком UDP/IP представлено на рисунке 2.20.

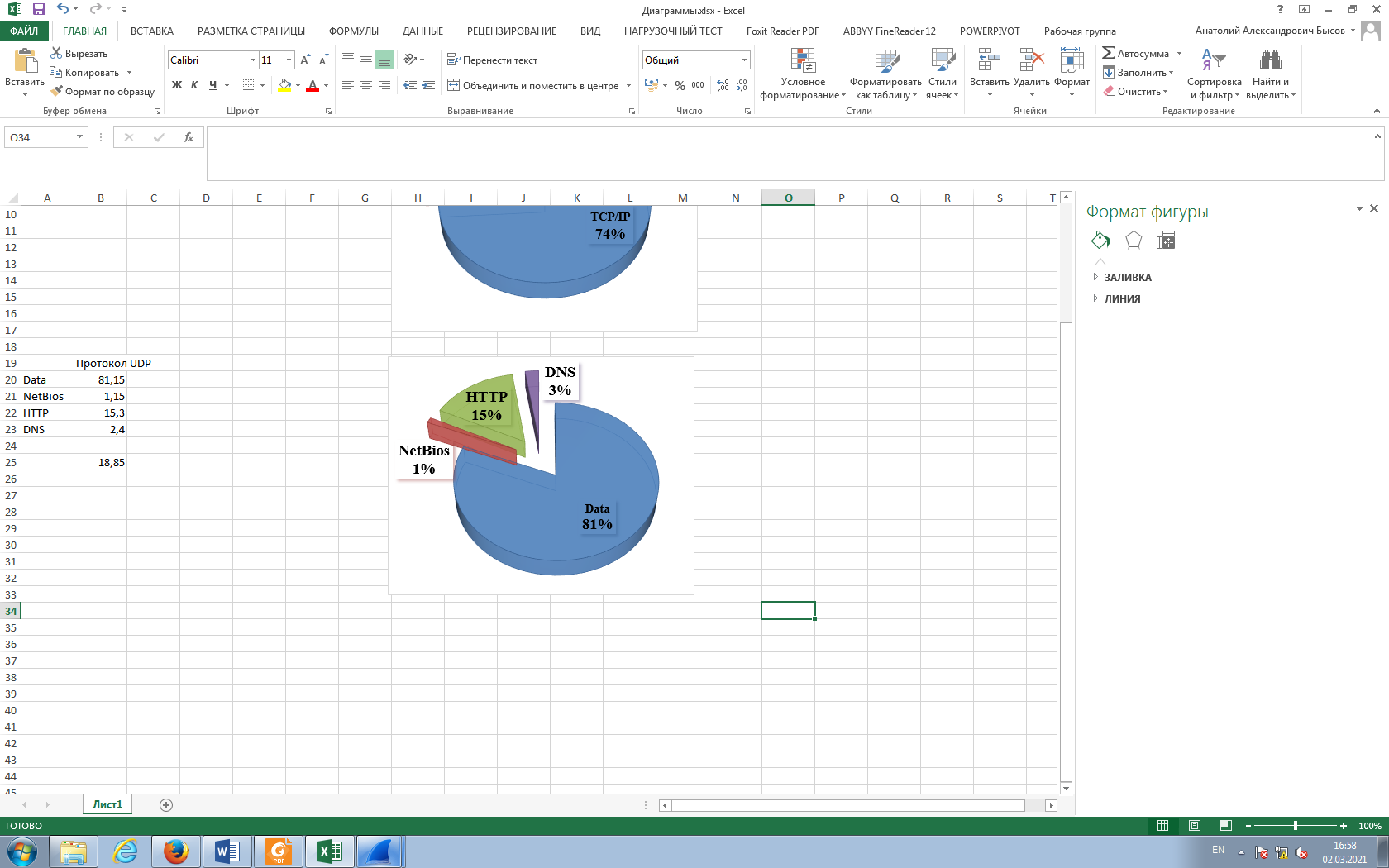


Рисунок 2.20 – Структура трафика в соответствии со стеком протоколов UDP/IP

На рисунке 2.20 показано, что 81% занимают передаваемые данные, к которым относится подвижное изображение (видеопоток), голосовая информация. Данный видео и аудио поток формируют IP-камеры системы видеонаблюдения. Следующим по объему является трафик, переданный в соответствии с протоколом HTTP (15%).

Протокол HTTP (Hypertext Transfer Protocol) является протоколом прикладного уровня ЭМВОС. Данный протокол используется для работы с веб-ресурсами. Основной программой для работы в соответствии с протоколом HTTP на стороне клиента является веб-браузер. В исследуемой корпоративной мультисервисной сети сотрудники пользуются доступом в сеть Интернет, а также доступом к корпоративному сайту, размещенного на веб-сервере. Процесс обмена в системе «клиент-сервер» в соответствии с протоколом HTTP представлено на рисунке 2.21.

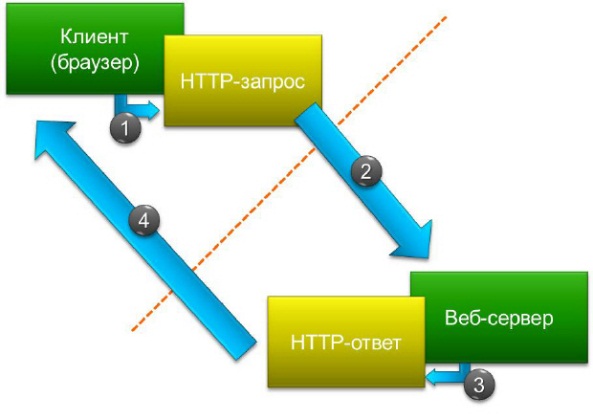


Рисунок 2.21 – Процесс обмена в соответствии с протоколом HTTP

Протокол DNS (Domain Name System – система доменных имен). Протокол прикладного уровня ЭМВОС, который предназначен для преобразования известного доменного имени (например, mail.ru) в IP-адрес сервера, на котором находится веб-ресурс. Организация работы службы DNS представлена на рисунке 2.22.

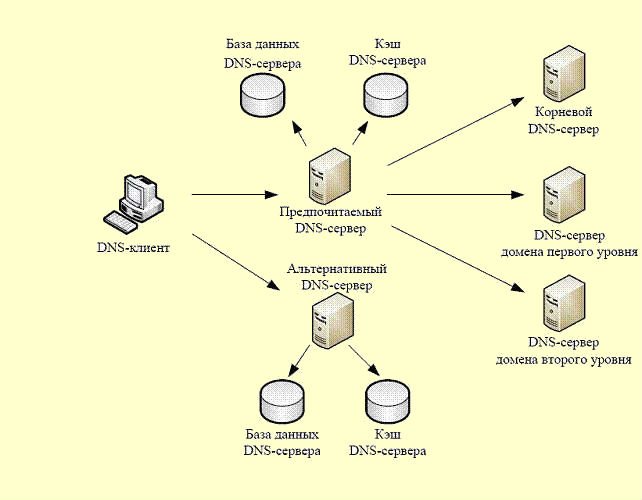


Рисунок 2.22 – Организация службы DNS

Протокол NetBIOS (Network Basic Input/Output System) – протокол сеансового уровня ЭМВОС, разработанный для локальных вычислительных сетей, построенных на базе компьютеров семейства IBM/PC. Является универсальным протоколом-интерфейсом взаимодействия (API) для управления сетевыми операциями ввода/вывода.

Распределение пакетов в соответствии со стеком TCP/IP представлено на рисунке 2.23.

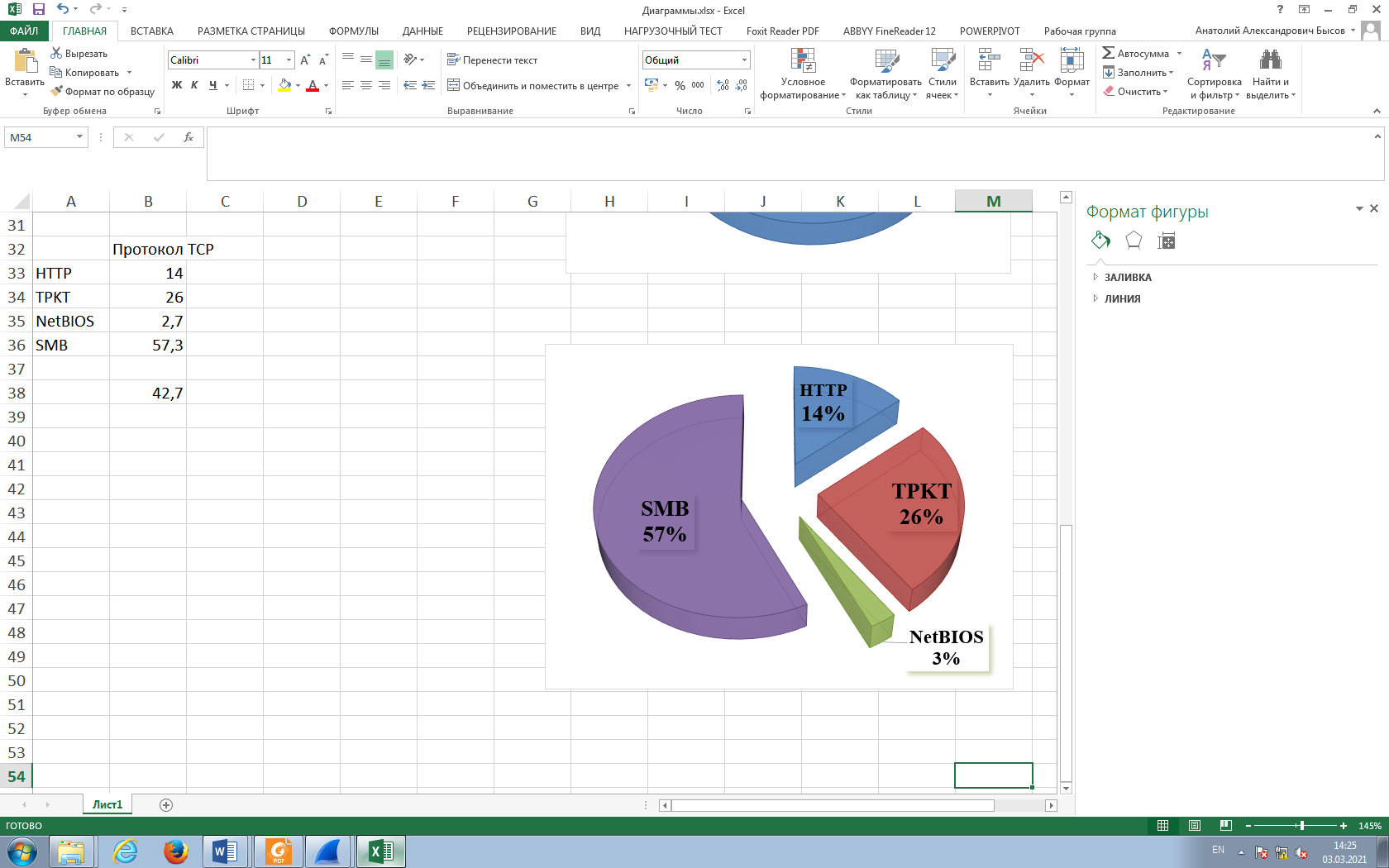


Рисунок 2.23 – Структура трафика в соответствии со стеком протоколов TCP/IP

На рисунке 2.20 показано, что 57% занимают пакеты, переданные в соответствии с протоколом SMB (Server Message Block) – протокол сетевого уровня ЭМВОС, который обеспечивает доступ к сетевым ресурсам: файлам, принтерам, сканерам, а также для межпроцессорного взаимодействия.

Протокол HTTP также может передаваться в соответствии с протоколом транспортного уровня TCP, о чем свидетельствует статистика в результате регистрации мультисервисного трафика. Похожая ситуация и с протоколом NetBIOS (3%), который также поддерживает оба протокола транспортного уровня.

Протокол TPKT сеансовый протокол контроля передачи для протокола прикладного уровня RDP (Remote Desktop Protocol) – протокол удаленного рабочего стола. Данный протокол используется для обеспечения удаленной работы пользователей с сервером, на котором реализуется услуга терминальных подключений.

Дальнейший анализ проведен для длин пакетов, передаваемых в мультисервисной корпоративной сети. Диаграмма распределения длин пакетов в соответствии со стеком TCP/IP представлена на рисунке 2.24.

Большая часть пакетов в передаваемом трафике имеют длину в диапазоне от 40 до 319 байт. Средняя длина пакетов равна 302 байта.

Рисунок 2.24 – Диаграмма длин пакетов трафика в соответствии со стеком протоколов TCP/IP

Диаграмма распределения длин пакетов в соответствии со стеком UDP/IP представлена на рисунке 2.25.

Распределение длин пакетов в соответствии со стеком UDP/IP имеет более равномерную структуру. Средняя длина пакетов равна 871 байт.

Рисунок 2.25 – Диаграмма длин пакетов трафика в соответствии со стеком протоколов UDP/IP

Пакеты определенных протоколов прикладного уровня (например, UDP) имею более однородную структуру распределения длин пакетов (рисунок 2.26).

Рисунок 2.26 – Диаграмма длин пакетов трафика в соответствии со стеком протоколов HTTP/UDP/IP

Большинство пакетов (84%) имеют длину в диапазоне от 320 до 639 байт, что можно объяснить принципом работы протокола UDP. То есть, при негарантированной доставке пакетов и отсутствии логического соединения между отправителем и получателем, нет механизма изменения длин пакетов в зависимости от качества передачи по каналам связи.

Для сравнения проанализирован тот же протокол прикладного уровня (HTTP), но при передаче в соответствии со стеком TCP/IP (рисунок 2.27).

Рисунок 2.26 – Диаграмма длин пакетов трафика в соответствии со стеком протоколов HTTP/TCP/IP

На рисунке 2.26 показано, что протокол транспортного уровня управляет длиной сегмента в зависимости от условий передачи (например, пакеты с длиной в диапазоне от 320 до 639 байт отсутствуют).

Отдельно исследовано распределение длин пакетов в соответствии с протоколом ICMP (Internet Control Message Protocol) ‑ протокол межсетевых управляющих сообщений. Распределение длин пакетов в соответствии с протоколом ICMP представлено на рисунке 2.27.

Рисунок 2.27 – Диаграмма длин пакетов трафика в соответствии  
с протоколом ICMP

Пакеты протокола ICMP имеют фиксированную длину. Длина ICMP-пакета равна 74 байта.

Также проведено исследование пакетов, переданных в соответствии с протоколом ARP (Address Resolution Protocol) – протокола разрешения адресов. Распределение длин пакетов в соответствии с протоколом ARP представлено на рисунке 2.28. Средняя длина ARP-пакетов равна 58 байт.

Учитывая факт одновременной поддержки двух протоколов сетевого уровня (IPv4 и IPv6) на большинстве современных терминальных и сетевых устройств, проведен анализ распределения длин пакетов данных протоколов. Распределение длин пакетов в соответствии с протоколом IPv4 и IPv6 представлено на рисунках 2.29 и 2.30 соответственно.

Рисунок 2.28 – Диаграмма длин ARP-пакетов

Рисунок 2.29 – Диаграмма длин пакетов IPv4

Рисунок 2.30 – Диаграмма длин пакетов IPv6

Распределение длин пакетов в соответствии с протоколом IPv4 носит достаточно предсказуемый характер, а именно, большинство протоколов вышестоящих уровней (от транспортного до прикладного) используют на сетевом уровне протокол IP и определяют необходимую длину пакета на данном уровне. Средняя длина пакета IPv4 равна 434 байта.

Для пакетов IPv6 наблюдается иная картина (рисунок 2.30): распределение длин большинства пакетов соответствует диапазону от 80 до 159 байт, что можно объяснить небольшим количеством прикладных процессов, которые используют в качестве протокола сетевого уровня IPv6. Таким образом, применение шестой версии протокола IP в исследуемой корпоративной сети носит ограниченный характер. Средняя длин пакета IPv6 равна 134 байта.

**2.3 Выводы**

1. Рассматриваемая корпоративная мультисервисная сеть строится на достаточно низкоскоростной технологии SHDSL (в сравнении с волоконно-оптическими линиями связи).
2. В настоящей главе проведен сбор и анализ мультисервисного трафика при помощи программы WireShark. На основе данного программного продукта проведена оценка интенсивности трафика и средней интенсивности трафика.
3. Получены данные о структуре мультисервисного трафика на всех уровнях эталонной модели взаимодействия открытых систем. Определены соотношения доли различных протоколов в общей структуре трафика.
4. Проведен анализ распределения длин пакетов на сетевом и транспортном уровне, а также исследованы особенности передачи протокола HTTP в зависимости от используемого протокола транспортного уровня.