

Министерство образования Республики Беларусь  
Учреждение образования  
«Белорусский государственный университет  
информатики и радиоэлектроники»

Кафедра сетей и устройств телекоммуникаций

**М. Ю. Хоменок**

***СТРУКТУРА СООБЩЕНИЙ  
ПРОТОКОЛА SIP***

Методическое пособие  
к лабораторно-практическим занятиям по курсу  
«Сетевые технологии и сигнализация в телекоммуникациях»  
для студентов специальностей  
1-45 01 03 «Сети телекоммуникаций»,  
1-45 01 05 «Системы распределения мультимедийной информации»  
всех форм обучения

Минск БГУИР 2011

УДК 654.9+004.724.4(076)

ББК 32.885я73

X76

Р е ц е н з е н т:

доцент кафедры «Системы телекоммуникаций»  
учреждения образования «Белорусский государственный университет  
информатики и радиоэлектроники», кандидат технических наук  
В. Н. Урядов

**Хоменок, М. Ю.**

X76

Структура сообщений протокола SIP : метод. пособие к лаб.-  
практич. занятиям по курсу «Сетевые технологии и сигнализация в  
телекоммуникациях» для студ. спец. 1-45 01 03 «Сети  
телекоммуникаций» и 1-45 01 05 «Системы распределения  
мультимедийной информации» всех форм обуч. / М. Ю. Хоменок. –  
Минск : БГУИР, 2011. – 31 с. : ил.

ISBN 978-985-488-757-9.

Рассмотрены особенности лексической структуры сообщений протокола SIP,  
структуры диалога при установлении видеотелефонного соединения в  
трехэлементной модели сети SIP на основе программного сервера MSS и  
терминалов X-Lite (два приложения).

Пособие предназначено для выполнения лабораторно-практических занятий  
при изучении особенностей информационного взаимодействия на основе  
сообщений протокола SIP терминального и сетевого оборудования сетей передачи  
данных с пакетной коммутацией.

**УДК 654.9+004.724.4(076)**  
**ББК 32.885я73**

**ISBN 978-985-488-757-9**

© Хоменок М. Ю., 2011  
© УО «Белорусский государственный  
университет информатики  
и радиоэлектроники», 2011

## Цель работы

1. Изучение лексической структуры сообщений SIP в режимах регистрации, установления и завершения мультимедийной сессии с использованием модели SIP-сети на основе программного сервера MSS.

2. Приобретение практических навыков инсталляции программных терминалов X-Lite, анализа структуры пакетов при организации мультимедийной сессии с использованием анализатора трафика Wireshark.

## Домашнее задание

1. Описать структуру SIP-сети, общий формат сообщений запросов и ответов и типы адресации при установлении мультимедийных вызовов.

2. Изучить принципы построения SIP-сети на основе программного сервера MSS и программных терминалов X-Lite.

## Лабораторное задание

1. Выполнить настройки элементов SIP-сети на основе программного минисервера MSS и двух терминалов X-Lite.

2. Выполнить анализ маршрутной информации при реализации диалога между элементами сети с использованием анализатора трафика Wireshark в режимах регистрации, установления и завершения мультимедийной сессии.

## Краткие теоретические сведения

### 1. Построение модели сети SIP

Топология модели сети SIP представлена тремя компьютерами, объединенными локальной сетью по технологии Ethernet (рис. 1). Один компьютер выполняет роль прокси-сервера, сервера регистрации и сервера определения местоположения, а два других – роли клиентов сети SIP.

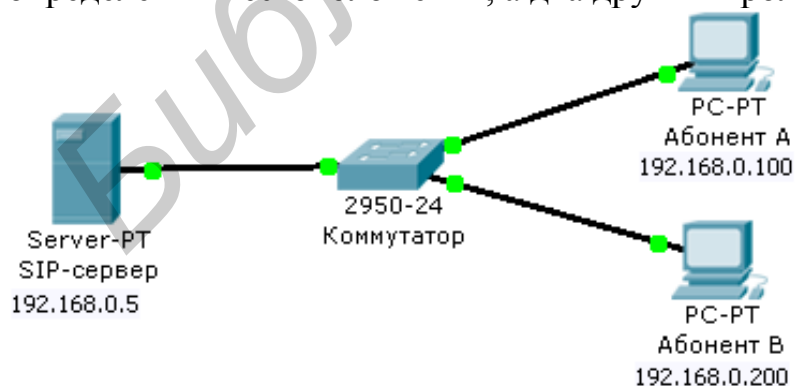


Рис. 1. Топология модели сети SIP

В качестве прокси-сервера используется программный продукт miniSipServer (MSS) компании MyVoipApp для таких систем Microsoft Windows, как Windows 2000/XP/2003/2008/Vista и Windows7. MSS основан на открытых стандартах SIP, которые поддерживаются большинством производителей оборудования IPTv и VoIP, выполняя функции сервера регистрации и прокси-сервера.

Основными характеристиками miniSipServer являются [1]:

- простота настройки посредством графического интерфейса GUI (Grafical User Interface – графический интерфейс пользователя);
- поддержка большинства аппаратных и программных SIP-телефонов различных производителей;
- возможность работы в локальной и во внешней сетях, в том числе возможность совершать звонки абонентам ТФОП, используя медиашлюз;
- поддержка CDR (Call Detail Record – записи о вызовах пользователей) при начислении платы за звонки и системного «черного» списка;
- поддержка функций STUN-сервера для выполнения трансляции адреса. STUN-сервер – это сетевой протокол, позволяющий клиенту, находящемуся за сервером трансляции адресов, определить свой внешний IP-адрес и порт во внешней сети, связанный с определенным внутренним номером порта. Эта информация используется для установления соединения UDP между двумя хостами, в случае если они оба находятся за маршрутизаторами NAT;
- поддержка мощных планов вызовов, гибкой маршрутизации вызовов, в том числе к другому SIP-серверу или MSS, различных видов переадресации, в том числе при помощи оператора;
- возможность оставить голосовое сообщение посредством голосовой почты при занятости или недоступности вызываемого абонента;
- поддержка групповых вызовов, удержание линии, повторного вызова, мгновенных сообщений (instant messages);
- возможность сигнализации абонентам при появлении в сети определенного пользователя;
- поддержка автоответчика, перехвата вызова/группы вызовов, удаленной базы данных абонентов и различных видов оплаты за вызов.

## 2. Настройка серверов MSS для работы с SIP-терминалами

При запуске сервер автоматически определяет IP-адрес компьютера, на

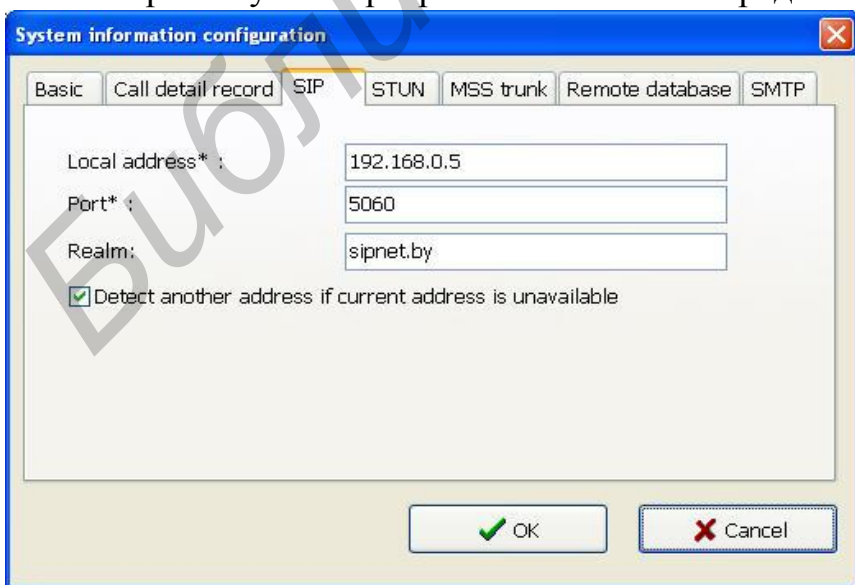


Рис. 2. Пример конфигурации MSS для работы с SIP

котором он установлен, и использует его как свой собственный при настройке SIP-сервера, а также для настройки протокола STUN.

По умолчанию MSS использует порт 5060 для установления соединений по протоколу SIP, однако при необходимости эти настройки могут быть изменены (рис. 2).

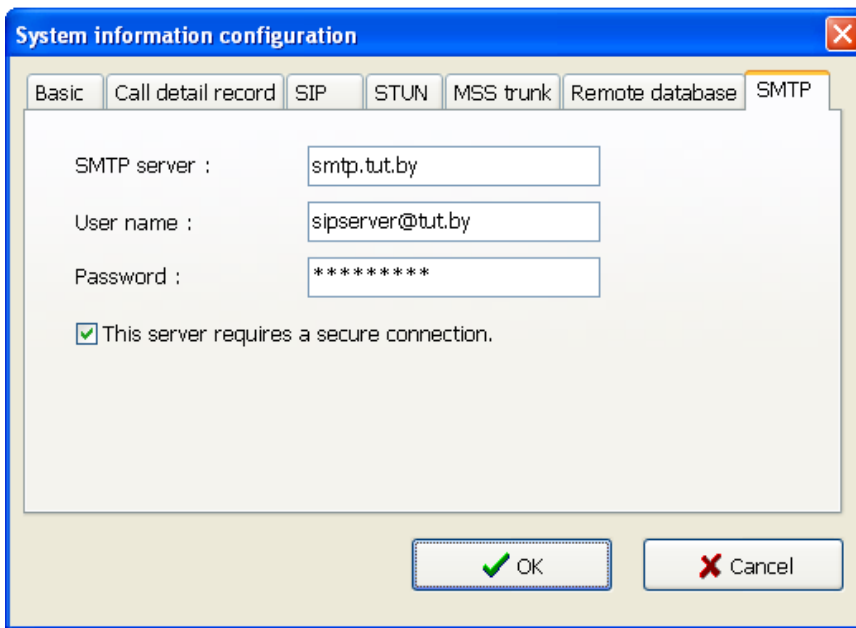


Рис. 3. Пример конфигурации MSS для работы с SMTP

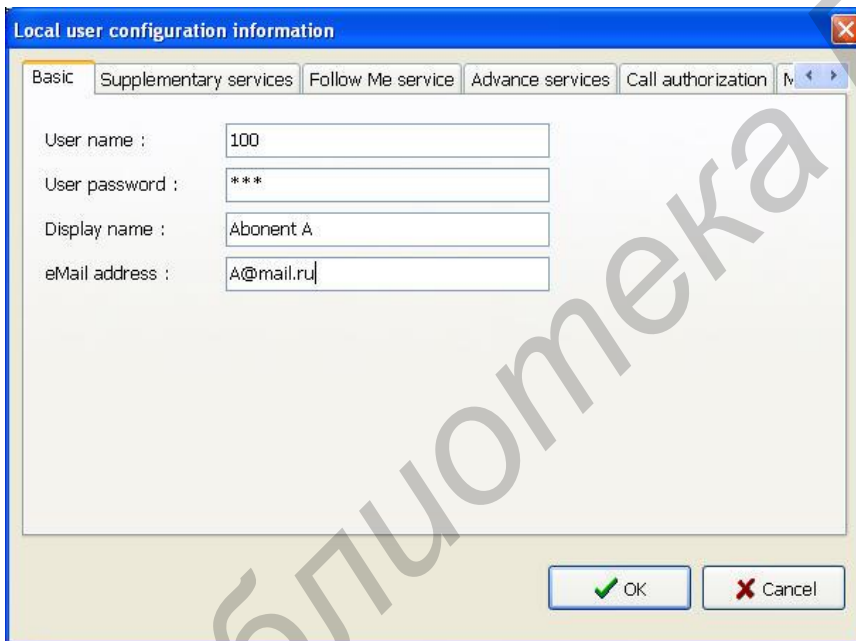


Рис. 4. Пример формирования учетной записи

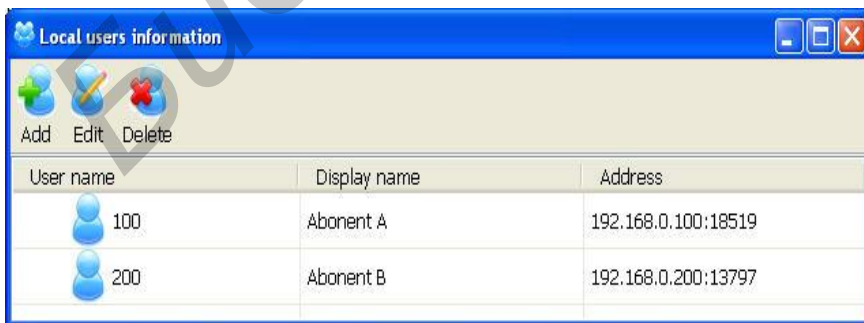


Рис. 5. Локальные пользователи

Для поддержки функции «голосовая почта» необходимо настроить сетевой протокол SMTP (Simple Mail Transfer Protocol – простой протокол передачи почты), предназначенный для передачи электронной почты в сетях TCP/IP (рис. 3).

Для взаимодействия пользователей между собой должна быть произведена их регистрация на сервере.

Для этого в главном окне нужно выбрать вкладку «Local users», затем – «Add» и заполнить соответствующие поля: номер, пароль, дисплейное имя и адрес почты вызываемого абонента (рис. 4).

После того как добавлены все пользователи, обслуживание указанных абонентов сервером будет производиться только в пределах локальной сети (рис. 5).

Если есть необходимость осуществления звонков в другие сети, нужно настроить хотя бы одну внешнюю линию (external line) (рис. 6).

### 3. Настройка терминала SIP для работы с сервером MSS

В качестве клиентов сети используется программный телефон (softphone) X-Lite 3.0 компании CounterPath Solutions, Inc для систем Microsoft Windows, таких, как Windows 2000/XP/2003/2008/Vista и Windows7 (рис. 7). Основанный на открытых стандартах SIP X-Lite предлагает производство традиционной телефонии в сочетании с возможностями настольных и мобильных компьютеров. С помощью простого нажатия клавиши мыши или клавиатуры пользователь может совершить звонок, принять вызов или управлять им.



Рис. 6. Пример конфигурации внешней линии сервера MSS



Рис. 7. Главное окно SIP-терминала X-Lite

Основными характеристиками программного терминала X-Lite являются [2]:

- наличие экрана вызова и индикатора ожидания сообщения;
- поддержка функций ДВО (громкой связи (спикерфон), отключения звука (mute), повторного вызова, удержания линии, режима «не беспокоить», игнорирования вызова, истории вызовов в виде списка принятых, пропущенных, совершенных и заблокированных вызовов, переадресации, трехсторонних аудио- и видеоконференций, мгновенных сообщений (instant messaging));
- поддержка двух линий связи, возможности сигнализации другим абонентам в сети при появлении пользователя при помощи протокола SIMPLE, управляемого списка контактов;

- поддержка технологии Intel® Centrino® Mobile, позволяющей X-Lite предоставлять более высокое качество обслуживания в проводных и беспроводных сетях, используя промышленные стандарты, такие, как 802.11e;
- не требует ручной настройки аудио- и видеоустройств;
- автоматическое определение полосы пропускания, которую может получить пользовательский компьютер для установления соединения;
- подавление эхо, автоматический контроль усиления, определение голосовой активности;
- поддержка следующих аудиокодеков: Broadvoice-32, Broadvoice-32 FEC, G.711aLaw, G.711uLaw, GSM, iLBC, L16 PCM Wideband, DVI4, DVI4 Wideband, Speex, Speex FEC, Speex Wideband, Speex Wideband FEC;
- поддержка следующих видеокодеков: H.263, H.263+.
- автоматический выбор наилучшего кодека на основании возможностей удаленной стороны, доступной полосы пропускания и состояния сети; X-Lite выбирает кодеки во время соединения в ответ на изменения состояния сети;
- совместимость со стандартами SIP, описанными в RFC 3261;
- поддержка протоколов STUN и ICE NAT для работы при нахождении за сервером трансляции адресов; поддержка протокола XTunnels для работы при нахождении за сетевым экраном (firewall);
- поддержка DTMF (RFC 2833 – внутриполосный DTMF) или сообщения SIP INFO.

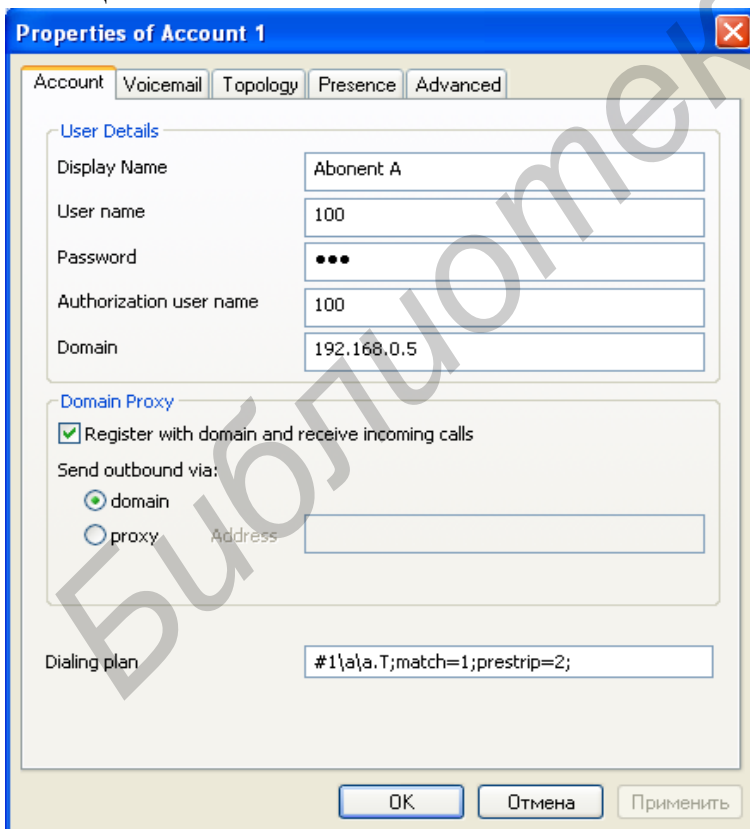


Рис. 8. Настройка SIP-клиента X-Lite

Для настройки клиента X-Lite необходимо выполнить следующие операции. После запуска программы X-Lite нужно нажать правую клавишу мыши и выбрать «SIP Account Settings...». В появившемся окне нажать «Add» и заполнить соответствующие поля, причем поля «User name» и «Password» должны соответствовать тем, которые присутствуют в учетной записи на сервере (рис. 8).

В поле «Domain» должен стоять ip-адрес SIP-сервера или его доменное имя.

После произведенных настроек SIP-клиент

видеотерминала готов для обслуживания вызовов.

#### *4. Настройка анализатора трафика Wireshark*

Анализ нагрузки, создаваемой протоколом SIP и мультимедийным трафиком, выполняется программным анализатором трафика Wireshark. Wireshark работает на основе библиотеки Pcap (Packet Capture). Для Unix-подобных систем используют libpcap-библиотеку, а для Microsoft Windows NT используют WinPcap-библиотеку.

Функциональные возможности анализатора пакетов Wireshark обеспечивают [3]:

- работу с большинством современных операционных систем (Microsoft Windows, Mac OS X, UNIX);

- перехват трафика сетевого интерфейса в режиме реального времени с интерфейсов Ethernet, IEEE 802.11, PPP/HDLC, ATM, Bluetooth, USB, Token Ring, Frame Relay, FDDI и других в зависимости от используемой платформы;

- быстрый захват и автономный анализ полученной информации;

- поддержку многих протоколов с добавлением новых возможностей (TELNET, FTP, POP, RLOGIN, ICQ, SMB, MySQL, HTTP, NNTP, X11, NAPSTER, IRC, RIP, BGP, SOCKS 5, IMAP 4, VNC, LDAP, NFS, SNMP, MSN, YMSG и др.);

- расшифровку таких протоколов, как IPsec, ISAKMP, Kerberos, SNMPv3, SSL/TLS, WEP, and WPA/WPA2;

- анализ мультимедийных пакетов VoIP и IPTv;

- сохранение и открытие ранее перехваченного сетевого трафика в формате XML, PostScript, CSV или просто текста;

- импорт и экспорт файлов из других пакетных анализаторов;

- фильтрацию пакетов по множеству критериев;

- возможность устанавливать цвет различным типам данных для наглядного интуитивного анализа;

- создание разнообразной статистики.

Для настройки анализатора Wireshark для захвата пакетов протокола SIP необходимо выполнить следующие операции.

После запуска программы активируются окна «Capture», а затем – «Options».

В появившемся окне поля заполняются следующим образом:

- в поле «Interface» выбирается сетевой интерфейс, с которого будет производиться захват пакетов;

- в поле «Capture Filter:» записывается значение «udp port 5060», чтобы программа отбирала только пакеты протокола SIP;

- для запуска работы анализатора нажимается кнопка «Start».

#### *5. Процедура регистрации пользователей на сервере*

При подключении абонента А к сети выполняется процедура его регистрации на сервере. Выполнение этой процедуры иллюстрирует рис. 9.



No. -	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.0.100	192.168.0.5	SIP	Request: REGISTER sip:192.168.0.5
2	0.000480	192.168.0.5	192.168.0.100	SIP	Status: 407 Proxy Authentication Required (0 bindings)
3	0.204014	192.168.0.100	192.168.0.5	SIP	Request: REGISTER sip:192.168.0.5
4	0.205172	192.168.0.5	192.168.0.100	SIP	Status: 200 OK (1 bindings)

Рис. 9. Регистрация абонента А на сервере

Процесс регистрации абонента А представляется в виде трейса обмена сигнальными сообщениями между терминалом абонента А и сервером, показанным на рис. 10.

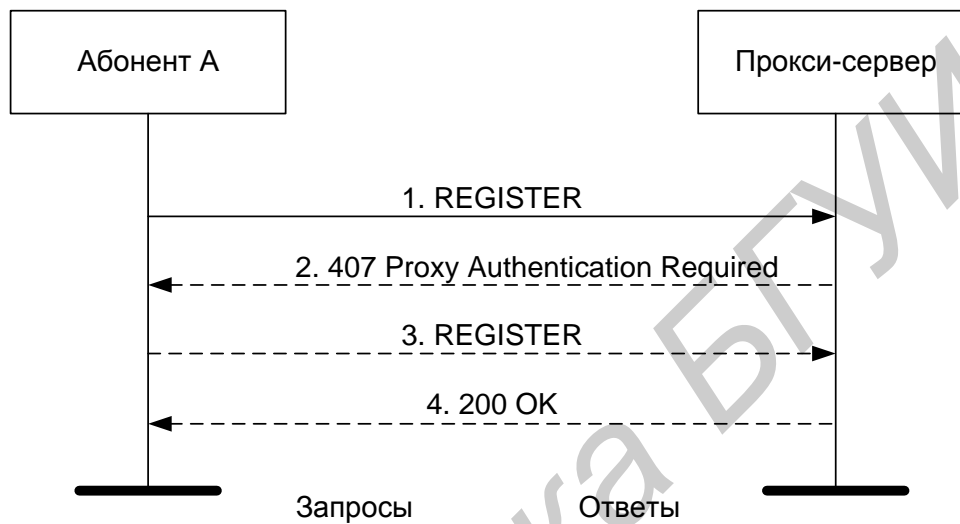


Рис. 10. Регистрация абонента А

Как видно из рис. 9 и 10, абонент А пытается зарегистрироваться дважды. Однако сервер отклоняет первую попытку и запрашивает аутентификацию абонента. После этого клиент пользователя посылает обновленный запрос регистрации, который включает необходимые для аутентификации данные. Сервер обрабатывает полученную информацию и высылает ответ «200 OK», что означает успешное прохождение процедуры регистрации. С этого момента клиент готов к работе.

На рис. 11 приведен текст запроса REGISTER, извлеченный из захваченного программой Wireshark пакета.

При помощи команды REGISTER пользователи сообщают свое текущее местоположение. В этом сообщении содержатся следующие заголовки маршрутной информации:

- заголовок Request-Line сообщает тип запроса (REGISTER), имя домена, в котором будет регистрироваться пользователь (sip:192.168.0.5), и версию протокола (SIP/2.0);

- заголовок Via содержит информацию обо всех узлах, через которые сообщение прошло прежде, чем было получено адресатом. В показанном примере эта информация совпадает с данными отправителя сообщения. В частности, указаны версия протокола SIP (SIP/2.0), протокол транспортного

уровня (UDP), IP-адрес и порт узла (192.168.0.100:38392); параметр «branch» означает, что на узле 192.168.0.100 запрос был размножен и направлен одновременно по разным направлениям. Данный запрос был передан по направлению, которое идентифицируется как z9hG4bK-d8754z-9221a04f4b0f6a4b-1---d8754z-. Значение поля Max-Forwards, равное 70, определяет максимальное количество узлов, через которые сообщение может пройти прежде, чем оно будет отброшено;

- заголовок To содержит адресную информацию, которую надо сохранить или модифицировать на сервере. В данном случае клиент «Abonent A» обращается к учетной записи с именем «100», хранящейся на сервере с IP-адресом 192.168.0.5;

- заголовок From содержит адрес инициатора регистрации. Зарегистрировать пользователя может другое лицо. В рассматриваемом случае информация в поле From совпадает с информацией в поле To, так как соответствующие значения полей извлекаются из настроек самого клиента;

- заголовок Call-ID – уникальный идентификатор сеанса связи, совпадающий во всех сообщениях, принадлежащих одному сеансу связи;

- заголовок Contact содержит новый контактный адрес пользователя, по которому должны посылаться все дальнейшие запросы INVITE. В данном случае это адрес sip:100@192.168.0.100:38392. Если в команде REGISTER поле Contact отсутствует, то регистрация остается неизменной. В случае отмены регистрации здесь размещается символ «\*»;

- заголовок CSeq – уникальный идентификатор запроса, относящегося к одному соединению. Он служит для корреляции запроса с ответом на него. Заголовок состоит из двух частей: натурального числа и типа запроса (REGISTER). Сервер должен проверять значение CSeq в каждом принимаемом запросе и считать запрос новым, если значение CSeq больше предыдущего;

- заголовок Expires указывает время в секундах, по истечении которого регистрация заканчивается. Если данное поле отсутствует, то по умолчанию назначается время – 1 ч, после которого регистрация завершается. Регистрацию можно также отменить посылкой сообщения REGISTER с полем Expires, которому присвоено значение «0», и соответствующим полем Contact;

- заголовок Allow содержит список типов запросов, поддерживаемых клиентом. В данном случае клиент поддерживает запросы: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, NOTIFY, MESSAGE, SUBSCRIBE, INFO;

- заголовок Proxy-Authorization содержит информацию, необходимую для правильной аутентификации пользователя на сервере. В частности, указывается имя пользователя (Abonent A), схема и метод аутентификации (Digest и MD5 соответственно). Параметр «realm» указывает агенту пользователя, к какому домену он принадлежит, а параметр «nonce value» – уникальная строка, которая генерируется на сервере в момент создания запроса аутентификации и должна совпадать с одноименной строкой в ответе пользователя;

- заголовок Digest Authentication Response содержит ответ агента пользователя на запрос аутентификации, посланный сервером. На основании значения этого поля сервер принимает решение о том, зарегистрировать пользователя или ответить отказом;
- заголовок User-Agent содержит информацию об агенте пользователя;
- заголовок Content-Length указывает на размер тела сообщения, посланного получателю, в байтах. Если его значение равно нулю, то тело сообщения отсутствует.

```

⊞ Frame 3 (774 bytes on wire, 774 bytes captured)
⊞ Ethernet II, Src: Wistron_98:a9:e5 (00:1f:16:98:a9:e5), Dst: CompalCo_f0:37:70 (00:16:d4:f0:37:70)
⊞ Internet Protocol, Src: 192.168.0.100 (192.168.0.100), Dst: 192.168.0.5 (192.168.0.5)
⊞ User Datagram Protocol, Src Port: 38392 (38392), Dst Port: sip (5060)
⊞ Session Initiation Protocol
  ⊞ Request-Line: REGISTER sip:192.168.0.5 SIP/2.0
    Method: REGISTER
    [Resent Packet: False]
  ⊞ Message Header
    ⊞ Via: SIP/2.0/UDP 192.168.0.100:38392;branch=z9hG4bK-d8754z-9221a04f4b0f6a4b-1---d8754z-;rport
      Transport: UDP
      Sent-by Address: 192.168.0.100
      Sent-by port: 38392
      Branch: z9hG4bK-d8754z-9221a04f4b0f6a4b-1---d8754z-
      RPort: rport
      Max-Forwards: 70
    ⊞ Contact: <sip:100@192.168.0.100:38392;rinstance=d24d9451c1111357>
      ⊞ Contact Binding: <sip:100@192.168.0.100:38392;rinstance=d24d9451c1111357>
        ⊞ URI: <sip:100@192.168.0.100:38392;rinstance=d24d9451c1111357>
    ⊞ To: "Abonent A"<sip:100@192.168.0.5>
      SIP Display info: "Abonent A"
      SIP to address: sip:100@192.168.0.5
    ⊞ From: "Abonent A"<sip:100@192.168.0.5>;tag=6e26b338
      SIP Display info: "Abonent A"
      SIP from address: sip:100@192.168.0.5
      SIP tag: 6e26b338
      Call-ID: MZAYYZMLZjFmMGE3YjgwYmQxMmJkZmMxNWEMTlkNGU.
    ⊞ CSeq: 2 REGISTER
      Sequence Number: 2
      Method: REGISTER
      Expires: 3600
      Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, NOTIFY, MESSAGE, SUBSCRIBE, INFO
    ⊞ Proxy-Authorization: Digest username="Abonent A",realm="sipnet.by",
      nonce="461d7cbb7dd008392ef15d6f0c715737",uri="sip:192.168.0.5",response="3db8b42b5cb4bf8230f980f7db53d85b"
      Authentication Scheme: Digest
      Username: "Abonent A"
      Realm: "sipnet.by"
      Nonce Value: "461d7cbb7dd008392ef15d6f0c715737"
      Authentication URI: "sip:192.168.0.5"
      Digest Authentication Response: "3db8b42b5cb4bf8230f980f7db53d85b"
      Algorithm: MD5
      User-Agent: X-Lite release 1104o stamp 56125
      Content-Length: 0
  
```

Рис. 11. Запрос REGISTER с параметрами аутентификации

Запрос аутентификации содержит аналогичные поля с учетом соответствующих изменений в структуре сообщения.

На рис. 12 показан текст ответа на запрос REGISTER, извлеченный из захваченного программой Wireshark пакета.

Из сравнения рис. 11 и 12 видно, что в тексте ответа значения соответствующих полей совпадают со значениями полей в тексте запроса. Тем самым клиент может убедиться в правильности интерпретации сервером адресованной ему информации.

```
⊕ Frame 4 (539 bytes on wire, 539 bytes captured)
⊕ Ethernet II, Src: CompalCo_f0:37:70 (00:16:d4:f0:37:70), Dst: Wistron_98:a9:e5 (00:1f:16:98:a9:e5)
⊕ Internet Protocol, Src: 192.168.0.5 (192.168.0.5), Dst: 192.168.0.100 (192.168.0.100)
⊕ User Datagram Protocol, Src Port: sip (5060), Dst Port: 38392 (38392)
⊕ Session Initiation Protocol
  ⊖ Status-Line: SIP/2.0 200 OK
    Status-Code: 200
    [Resent Packet: False]
  ⊖ Message Header
    ⊖ Via: SIP/2.0/UDP 192.168.0.100:38392;branch=z9hG4bK-d8754z-9221a04f4b0f6a4b-1---d8754z-
      Transport: UDP
      Sent-by Address: 192.168.0.100
      Sent-by port: 38392
      Branch: z9hG4bK-d8754z-9221a04f4b0f6a4b-1---d8754z-
    ⊖ From: "Abonent A"<sip:100@192.168.0.5>;tag=6e26b338
      SIP Display info: "Abonent A"
      SIP from address: sip:100@192.168.0.5
      SIP tag: 6e26b338
    ⊖ To: "Abonent A"<sip:100@192.168.0.5>;tag=3b6c3a47
      SIP Display info: "Abonent A"
      SIP to address: sip:100@192.168.0.5
      SIP tag: 3b6c3a47
    ⊖ CSeq: 2 REGISTER
      Sequence Number: 2
      Method: REGISTER
      Call-ID: MZAYzMLZjFmMGE3YjgwYmQxMmJkZmMxNWEMTlkNGU.
      Allow: REGISTER, INVITE, OPTIONS, ACK, CANCEL, BYE, REFER, SUBSCRIBE, NOTIFY, MESSAGE
      User-Agent: minisipserver v2.8.12 (50) Nov 19 2009
    ⊖ Contact: <sip:100@192.168.0.100:38392>
      ⊖ Contact Binding: <sip:100@192.168.0.100:38392>
        ⊕ URI: <sip:100@192.168.0.100:38392>
      Expires: 3600
      Content-Length: 0
```

Рис. 12. Ответ на запрос REGISTER

Объем трафика, которым обменялись агент пользователя и сервер в процессе регистрации, определяется четырьмя пакетами. Первый объемом 585 байт, второй – 624 байта, третий – 774 байта, четвертый – 539 байтов. Таким образом, суммарный объем трафика составляет 2522 байта.

Регистрация абонента В происходит аналогично процедуре регистрации абонента А с учетом соответствующих изменений в структуре сообщений. При этом затрачивается такое же количество трафика.

После окончания работы клиента происходит процедура отмены регистрации. Эта процедура полностью повторяет процесс регистрации с той разницей, что в поле Expires запроса REGISTER устанавливается нуль. В ответе на этот запрос в поле Expires также устанавливается нуль.

## 6. Процедура установления соединения SIP при обслуживании видеотелефонного вызова

Рис. 13 иллюстрирует обслуживание по протоколу SIP видеотелефонного вызова абонента А к абоненту В в фазе установления соединения, в фазе передачи мультимедийного трафика в виде передачи речевых и видеопакетов, в фазе разрушения соединений, выделенных другим фоном.

No. - Time	Source	Destination	Protocol	Info
1 0.000000	192.168.0.100	192.168.0.5	SIP/SDP	Request: INVITE sip:200@192.168.0.5, with session description
2 0.000252	192.168.0.5	192.168.0.100	SIP	Status: 407 Proxy Authentication Required
3 0.002814	192.168.0.100	192.168.0.5	SIP	Request: ACK sip:200@192.168.0.5
4 0.004005	192.168.0.100	192.168.0.5	SIP/SDP	Request: INVITE sip:200@192.168.0.5, with session description
5 0.005897	192.168.0.5	192.168.0.100	SIP	Status: 100 Trying
6 0.006334	192.168.0.5	192.168.0.200	SIP/SDP	Request: INVITE sip:200@192.168.0.200:15552, with session description
7 0.113568	192.168.0.200	192.168.0.5	SIP	Status: 100 Trying
9 0.123005	192.168.0.200	192.168.0.5	SIP	Status: 180 Ringing
10 0.123571	192.168.0.5	192.168.0.100	SIP	Status: 180 Ringing
11 2.028636	192.168.0.200	192.168.0.5	SIP/SDP	Status: 200 OK, with session description
12 2.028888	192.168.0.5	192.168.0.200	SIP	Request: ACK sip:200@192.168.0.200:15552
13 2.029537	192.168.0.5	192.168.0.100	SIP/SDP	Status: 200 OK, with session description
14 2.148156	192.168.0.100	192.168.0.5	SIP	Request: ACK sip:200@192.168.0.5
15 5.068373	192.168.0.100	192.168.0.5	SIP/SDP	Request: INVITE sip:200@192.168.0.5, with session description
16 5.069729	192.168.0.5	192.168.0.100	SIP	Status: 100 Trying
17 5.069930	192.168.0.5	192.168.0.200	SIP/SDP	Request: INVITE sip:200@192.168.0.200:15552, with session description
18 5.182245	192.168.0.200	192.168.0.5	SIP/SDP	Status: 200 OK, with session description
19 5.182478	192.168.0.5	192.168.0.200	SIP	Request: ACK sip:200@192.168.0.200:15552
20 5.182701	192.168.0.5	192.168.0.100	SIP/SDP	Status: 200 OK, with session description
21 5.292033	192.168.0.100	192.168.0.5	SIP	Request: ACK sip:200@192.168.0.5
23 15.252090	192.168.0.100	192.168.0.5	SIP	Request: BYE sip:200@192.168.0.5
24 15.254302	192.168.0.5	192.168.0.100	SIP	Status: 200 OK
25 15.256159	192.168.0.5	192.168.0.200	SIP	Request: BYE sip:200@192.168.0.200:15552
26 15.362149	192.168.0.200	192.168.0.5	SIP	Status: 200 OK

■ Фаза установления соединения   ■ Модификация соединения   ■ Разрыв соединения

Рис.13. Видеотелефонный вызов абонента А абоненту В

Схематически процесс совершения видеовызова можно представить в виде, показанном на рис.14.

Как и в случае регистрации абонента на сервере, первый запрос сервер отклоняет и требует аутентификации пользователя. Клиент пользователя включает необходимую для прохождения аутентификации информацию во все последующие сообщения.

Запрос типа INVITE на этапе установления соединения с включенной в состав сообщения информацией для аутентификации представлен на рис. 15.

Маршрутные заголовки, которые содержатся в сообщениях протокола SIP, рассмотрены ранее на примере запроса типа REGISTER. В сообщении INVITE эти поля имеют такую же смысловую нагрузку. Информационная часть запроса INVITE включена в тело сообщения SIP и содержит описание сеанса связи в формате протокола SDP (Session Description Protocol – протокол

описания сессии). Протокол SDP описывает параметры мультимедиа сеанса связи и используется для объявления типа и параметров сессии в приглашении к началу сеанса связи и в других мультимедийных сеансах при установлении связи и согласовании параметров.

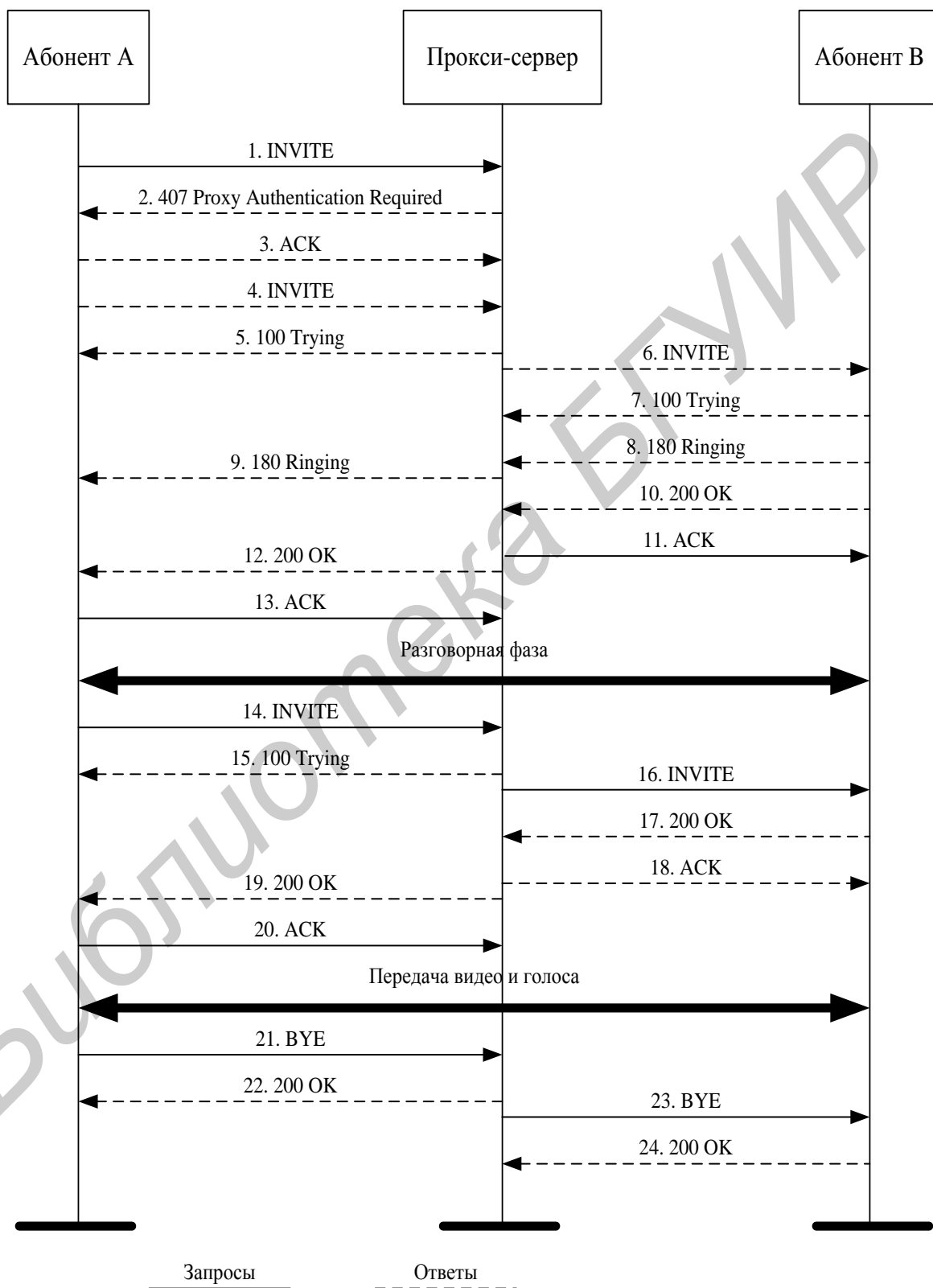


Рис. 14. Процедура установления видеотелефонного соединения

```

⊕ Frame 4 (1030 bytes on wire, 1030 bytes captured)
⊕ Ethernet II, Src: WISTRON_98:a9:e5 (00:1f:16:98:a9:e5), Dst: Compalco_f0:37:70 (00:16:d4:f0:37:70)
⊕ Internet Protocol, Src: 192.168.0.100 (192.168.0.100), Dst: 192.168.0.5 (192.168.0.5)
⊕ User Datagram Protocol, Src Port: 18900 (18900), Dst Port: sip (5060)
⊕ Session Initiation Protocol
⊕ Request-Line: INVITE sip:200@192.168.0.5 SIP/2.0
⊕ Message Header
⊕ Via: SIP/2.0/UDP 192.168.0.100:18900;branch=z9hG4bK-d8754z-5875a02ec44d9908-1---d8754z-;rport
  Max-Forwards: 70
⊕ Contact: <sip:100@192.168.0.100:18900>
⊕ To: "200"<sip:200@192.168.0.5>
⊕ From: "Abonent A"<sip:100@192.168.0.5>;tag=857dc618
  Call-ID: ZjBjMTg2ODlhYzk3YzkwMjY2MDFmYmIwOWUyMGQzZTk.
⊕ CSeq: 2 INVITE
  Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, NOTIFY, MESSAGE, SUBSCRIBE, INFO
  Content-Type: application/sdp
⊕ Proxy-Authorization: Digest username="Abonent A",realm="sipnet.by",
  nonce="47816bab45ea7c3402ed79617c384686",uri="sip:200@192.168.0.5",response="f9a77c6def4172db16cb64b9194bca02"
  User-Agent: X-Lite release 1104o stamp 56125
  Content-Length: 267
⊕ Message Body
⊕ Session Description Protocol
  Session Description Protocol Version (v): 0
⊕ Owner/Creator, Session Id (o): - 1 2 IN IP4 192.168.0.100
  Owner Username: -
  Session ID: 1
  Session Version: 2
  Owner Network Type: IN
  Owner Address Type: IP4
  Owner Address: 192.168.0.100
  Session Name (s): CounterPath X-Lite 3.0
⊕ Connection Information (c): IN IP4 192.168.0.100
  Connection Network Type: IN
  Connection Address Type: IP4
  Connection Address: 192.168.0.100
⊕ Time Description, active time (t): 0 0
  Session Start Time: 0
  Session Stop Time: 0
⊕ Media Description, name and address (m): audio 41114 RTP/AVP 107 0 8 101
  Media Type: audio
  Media Port: 41114
  Media Proto: RTP/AVP
  Media Format: 107
  Media Format: ITU-T G.711 PCMU
  Media Format: ITU-T G.711 PCMA
  Media Format: 101
⊕ Media Attribute (a): alt:1 1 : 7ByLgwoC MrhDLZkQ 192.168.0.100 41114
  Media Attribute Fieldname: alt
  Media Attribute Value: 1 1 : 7ByLgwoC MrhDLZkQ 192.168.0.100 41114
⊕ Media Attribute (a): fmp:101 0-15
  Media Attribute Fieldname: fmp
  Media Format: 101
  Media format specific parameters: 0-15
⊕ Media Attribute (a): rtpmap:107 BV32/16000
  Media Attribute Fieldname: rtpmap
  Media Format: 107
  MIME Type: BV32
⊕ Media Attribute (a): rtpmap:101 telephone-event/8000
  Media Attribute Fieldname: rtpmap
  Media Format: 101
  MIME Type: telephone-event
  Media Attribute (a): sendrecv

```

Рис. 15. Запрос типа INVITE

Описание SDP-сессии содержит ряд текстовых строк в формате:

<тип>=<значение>, где первый элемент <тип> – чувствительный к регистру символ, а второй элемент <значение> – структурированный текст, формат которого зависит от первого элемента <тип>. Ни до, ни после знака "=" не должно быть пробелов.

Структура описания сессии в формате SDP имеет следующий вид:

- v= (версия протокола);
- o= (идентификатор сессии);
- s= (имя сессии);
- i=\* (информация о сессии);
- u=\* (описание URI);
- e=\* (адрес электронной почты);
- p=\* (номер телефона);
- c=\* (информация о соединении);
- b=\* (нуль или более строк информации о полосе пропускания);
- одно или более описаний времени ("t=" и "r=" линии):
  - а) t= (время продолжительности сессии);
  - б) r=\* (нуль или больше повторений);
- z=\* (согласование временной зоны);
- k=\* (ключ шифрования);
- a=\* (нуль или более строк с атрибутами сессии);
- нуль или более описаний медиа-контента:
  - а) m= (название медиа-контента и транспортный адрес);
  - б) i=\* (заголовок медиа-контента);
  - в) c=\* (информация о соединении);
  - г) b=\* (нуль или более строк информации о полосе пропускания);
  - д) k=\* (ключ шифрования);
  - е) a=\* (нуль или более строк с атрибутами сессии).

Структура тела сообщения, изображенного на рис. 15, соответствует общей структуре описаний протокола SDP.

Поле версии протокола SDP равно нулю, так как другие версии протокола не определены.

Поле Owner/Creator, Session Id – поле идентификатора сессии – содержит строку: «o= – 1 2 IN IP4 192.168.0.100». Прочерк означает, что вызывающий хост не поддерживает концепцию пользовательских имен; 1 – идентификатор сессии; 2 – версия сессии; IN – тип используемой сети, в данном случае Internet; IP4 – тип сетевого адреса, в данном случае используется IP-адрес версии четыре; 192.168.0.100 – IP-адрес вызывающего хоста.

Поле Session Name содержит название сессии: CounterPath X-Lite 3.0.

Поле Connection Information содержит информацию о соединении: IN IP4 192.168.0.100. IN – тип используемой сети, в данном случае Internet; IP4 – тип сетевого адреса, в данном случае используется IP-адрес версии четыре; 192.168.0.100 – IP-адрес вызывающего хоста.

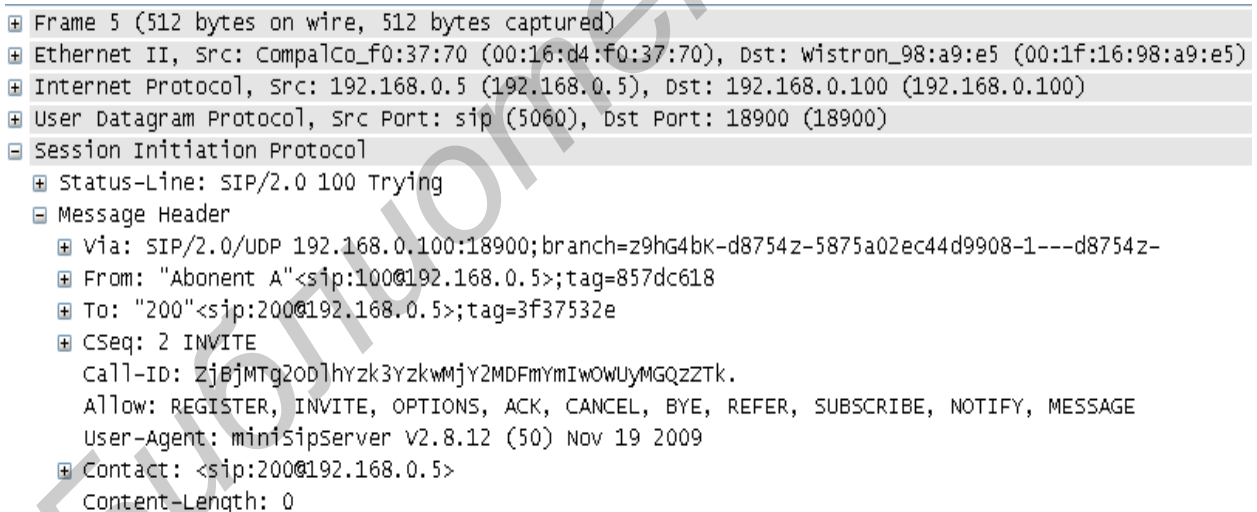


Поле Time Description содержит сведения о времени начала и окончания сессии. Отметка начала сессии равна нулю, что свидетельствует о постоянном характере сессии. Отметка конца также равна нулю, значит, сессия не ограничена во времени.

Поле атрибутов Media Description содержит описание свойств передаваемого трафика: audio 41114 RTP/AVP 107 0 8 101: Audio – тип трафика, в данном случае аудиотрафик; 41114 – номер порта, на который следует передавать указанный трафик; RTP/AVP – тип транспортного протокола, RTP с профилями аудио, видео (AVP); 107 0 8 101 – это описания форматов трафика, с которыми может работать вызывающий пользователь, 107 и 101 – динамические форматы, которые более полно определяются соответствующими полями rtpmap; 0 – это аудиокодек ITU-T G.711 PCMU; 8 – это аудиокодек ITU-T G.711 PCMA. Из этих четырех типов форматов трафика первый предлагается в качестве формата по умолчанию для сессии.

Поле Media Attribute (a): fntp определяет взаимодействие с DTMF. Содержание этого поля означает, что для формата трафика 101 возможно принимать события 0-15 с помощью DTMF-сигналов: 0-15 – это цифры от нуля до пятнадцати, 10 – «\*», 11 – «#», 12-15 – буквы от А до D.

Поле Media Attribute (a): rtpmap:107 уточняет формат трафика номер 107. Его содержание означает, что используется кодек BV32 (BroadVoice32) с частотой дискретизации 16 кГц и скоростью выходного потока 32 кбит/с. Это широкополосный кодек для передачи голоса высокого качества.



```

+ Frame 5 (512 bytes on wire, 512 bytes captured)
+ Ethernet II, Src: CompalCo_f0:37:70 (00:16:d4:f0:37:70), Dst: wistron_98:a9:e5 (00:1f:16:98:a9:e5)
+ Internet Protocol, Src: 192.168.0.5 (192.168.0.5), Dst: 192.168.0.100 (192.168.0.100)
+ User Datagram Protocol, Src Port: sip (5060), Dst Port: 18900 (18900)
- Session Initiation Protocol
  + Status-Line: SIP/2.0 100 Trying
  - Message Header
    + Via: SIP/2.0/UDP 192.168.0.100:18900;branch=z9hG4bK-d8754z-5875a02ec44d9908-1---d8754z-
    + From: "Abonent A"<sip:100@192.168.0.5>;tag=857dc618
    + To: "200"<sip:200@192.168.0.5>;tag=3f37532e
    + CSeq: 2 INVITE
      Call-ID: zjBjMTg2ODlhYzk3YzkwMjY2MDFmYmIwOWUyMGQzZTk.
      Allow: REGISTER, INVITE, OPTIONS, ACK, CANCEL, BYE, REFER, SUBSCRIBE, NOTIFY, MESSAGE
      User-Agent: minisipserver v2.8.12 (50) Nov 19 2009
    + Contact: <sip:200@192.168.0.5>
    Content-Length: 0

```

Рис. 16. Ответ 100 Trying

Поле Media Attribute (a): rtpmap:101 уточняет формат трафика номер 101. Его содержание означает, что это обычный телефонный кодек с частотой дискретизации 8кГц.

Поле Media Attribute (a): sendrecv означает, что клиент должен быть запущен в режиме приема и передачи. Это необходимо для интерактивных конференций с клиентами, которые по умолчанию находятся только в принимающем режиме.

В ответ на запрос INVITE прокси-сервер посылает ответ 100 Trying. Это означает, что запрос принят и обрабатывается. Этот ответ представлен на рис. 16. Видно, что ответ содержит стандартные поля сообщений протокола SIP.

Запрос INVITE передается прокси-сервером вызываемому абоненту. Последний высылает ответ 100 Trying. Далее в сторону прокси-сервера следует ответ 180 Ringing, который является аналогом контроля посылки вызова в обычной телефонии. Пример этого ответа представлен на рис. 17.

```
⊕ Frame 9 (414 bytes on wire, 414 bytes captured)
⊕ Ethernet II, Src: Inventec_54:78:9f (00:1e:33:54:78:9f), Dst: CompalCo_f0:37:70 (00:16:d4:f0:37:70)
⊕ Internet Protocol, Src: 192.168.0.200 (192.168.0.200), Dst: 192.168.0.5 (192.168.0.5)
⊕ User Datagram Protocol, Src Port: 15552 (15552), Dst Port: sip (5060)
⊕ Session Initiation Protocol
  ⊕ Status-Line: SIP/2.0 180 Ringing
  ⊕ Message Header
    ⊕ Via: SIP/2.0/UDP 192.168.0.5:5060;branch=z9hG4bK-3b085e09-4c050e1d-43a9430
    ⊕ Contact: <sip:200@192.168.0.200:15552>
    ⊕ To: "200"<sip:200@192.168.0.5>;tag=074a0306
    ⊕ From: "Абонент А"<sip:100@192.168.0.5>;tag=399b4ea7
      Call-ID: 280c3b2ae80fc16c52122a-35483888@192.168.0.5
    ⊕ CSeq: 1 INVITE
      User-Agent: X-Lite release 1103k stamp 53621
      Content-Length: 0
```

Рис. 17. Ответ 180 Ringing

Ответ 180 Ringing несет минимальную смысловую нагрузку и информирует вызывающего пользователя и прокси-сервер о том, что вызываемый абонент получает звуковой сигнал от своего агента. Прокси-сервер пересылает ответ 180 Ringing вызываемому абоненту.

Когда вызываемый абонент принимает вызов, он отвечает сигналом 200 ОК, представленным на рис. 18. В ответе содержится информация о том, какие параметры сессии поддерживаются вызываемым пользователем. Если параметры сессии, содержащиеся в запросе INVITE, поддерживаются вызываемым абонентом, то эти параметры копируются из запроса INVITE в ответ 200 ОК. Именно такая ситуация изображена на рис. 18. Единственное отличие – это номер порта, на который вызываемый агент будет принимать мультимедийную информацию.

Сообщение 200 ОК подтверждается сигналом АСК (рис. 19). Так же как ответы 100 Trying и 180 Ringing, запрос АСК не содержит тела сообщения, т.е. несет минимальную смысловую нагрузку и просто подтверждает успешную обработку запроса вызываемым абонентом.

Прокси-сервер пересылает ответ 200 ОК вызываемому пользователю и получает от него подтверждение в виде сигнала АСК. После этого устанавливается разговорная фаза.

Если пользователь А желает осуществить видеосвязь с абонентом В, то он нажимает кнопку START в клиенте X-Lite.

- ⊕ Frame 11 (792 bytes on wire, 792 bytes captured)
- ⊕ Ethernet II, Src: Inventec\_54:78:9f (00:1e:33:54:78:9f), Dst: Compa|Co\_f0:37:70 (00:16:d4:f0:37:70)
- ⊕ Internet Protocol, Src: 192.168.0.200 (192.168.0.200), Dst: 192.168.0.5 (192.168.0.5)
- ⊕ User Datagram Protocol, Src Port: 15552 (15552), Dst Port: sip (5060)
- ⊕ Session Initiation Protocol
  - ⊕ Status-Line: SIP/2.0 200 OK
  - ⊕ Message Header
    - ⊕ Via: SIP/2.0/UDP 192.168.0.5:5060;branch=z9hG4bK-3b085e09-4c050e1d-43a9430
    - ⊕ Contact: <sip:200@192.168.0.200:15552>
    - ⊕ To: "200"<sip:200@192.168.0.5>;tag=074a0306
    - ⊕ From: "Abonent A"<sip:100@192.168.0.5>;tag=399b4ea7  
Call-ID: 280c3b2ae80fc16c52122a-35483888@192.168.0.5
    - ⊕ CSeq: 1 INVITE  
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, NOTIFY, MESSAGE, SUBSCRIBE, INFO  
Content-Type: application/sdp  
User-Agent: X-Lite release 1103k stamp 53621  
Content-Length: 267
  - ⊕ Message Body
    - ⊕ Session Description Protocol
      - Session Description Protocol Version (v): 0
      - ⊕ Owner/Creator, Session Id (o): - 1 2 IN IP4 192.168.0.200  
Owner Username: -  
Session ID: 1  
Session Version: 2  
Owner Network Type: IN  
Owner Address Type: IP4  
Owner Address: 192.168.0.200  
Session Name (s): CounterPath X-Lite 3.0
      - ⊕ Connection Information (c): IN IP4 192.168.0.200  
Connection Network Type: IN  
Connection Address Type: IP4  
Connection Address: 192.168.0.200
      - ⊕ Time Description, active time (t): 0 0  
Session Start Time: 0  
Session Stop Time: 0
      - ⊕ Media Description, name and address (m): audio 50768 RTP/AVP 107 0 8 101  
Media Type: audio  
Media Port: 50768  
Media Proto: RTP/AVP  
Media Format: 107  
Media Format: ITU-T G.711 PCMU  
Media Format: ITU-T G.711 PCMA  
Media Format: 101
      - ⊕ Media Attribute (a): alt:1 1 : NWFMRGwg ch5BRX6W 192.168.0.200 50768  
Media Attribute Fieldname: alt  
Media Attribute Value: 1 1 : NWFMRGwg ch5BRX6W 192.168.0.200 50768
      - ⊕ Media Attribute (a): fmp:101 0-15  
Media Attribute Fieldname: fmp  
Media Format: 101  
Media format specific parameters: 0-15
      - ⊕ Media Attribute (a): rtpmap:107 BV32/16000  
Media Attribute Fieldname: rtpmap  
Media Format: 107  
MIME Type: BV32
      - ⊕ Media Attribute (a): rtpmap:101 telephone-event/8000  
Media Attribute Fieldname: rtpmap  
Media Format: 101  
MIME Type: telephone-event  
Media Attribute (a): sendrecv

Рис. 18. Ответ 200 OK

В ответ на это событие агент клиента пользователя А передает прокси-серверу модифицированный запрос INVITE, изображенный на рис. 20.

При сравнении рис. 15 и 20 видно, что информация из первоначального запроса копируется в модифицированный и добавляются новые медиа-атрибуты.

```
⊕ Frame 12 (409 bytes on wire, 409 bytes captured)
⊕ Ethernet II, Src: CompalCo_f0:37:70 (00:16:d4:f0:37:70), Dst: Inventec_54:78:9f (00:1e:33:54:78:9f)
⊕ Internet Protocol, Src: 192.168.0.5 (192.168.0.5), Dst: 192.168.0.200 (192.168.0.200)
⊕ User Datagram Protocol, Src Port: sip (5060), Dst Port: 15552 (15552)
⊕ Session Initiation Protocol
  ⊕ Request-Line: ACK sip:200@192.168.0.200:15552 SIP/2.0
  ⊕ Message Header
    ⊕ Via: SIP/2.0/UDP 192.168.0.5:5060;branch=z9hG4bK-22867497-4c050e1f-577f3ac
    ⊕ To: "200"<sip:200@192.168.0.5>;tag=074a0306
    ⊕ From: "100"<sip:100@192.168.0.5>;tag=399b4ea7
      Call-ID: 280c3b2ae80fc16c52122a-35483888@192.168.0.5
      User-Agent: minisipserver v2.8.12 (50) Nov 19 2009
    ⊕ CSeq: 1 ACK
      Max-Forwards: 70
      Content-Length: 0
```

Рис.19. Запрос ACK

Поле атрибутов Media Description содержит описание свойств передаваемого трафика: video 37610 RTP/AVP 115 34. Video – тип трафика, видеотрафик в данном случае; 37610 – номер порта, на который следует передавать указанный трафик; RTP/AVP – тип транспортного протокола, RTP с профилями аудио, видео (AVP); 115 34 – это описания форматов трафика, с которыми может работать вызывающий пользователь, 115 – динамический формат, который более полно определяется соответствующим полем rtpmap; 34 – это видекодек ITU-T H.263. Из этих двух типов форматов трафика первый предлагается в качестве формата по умолчанию для сессии.

Поле Media Attribute (a): fmtp:115 уточняет формат 115.

Строка QCIF=1;CIF=1;I=1;J=1;T=1 означает поддержку этим форматом следующих атрибутов:

– QCIF (Quarter Common Intermediate Format) – видеоформат, используемый при видеоконференциях, который выдает видеопоток в тридцать кадров в секунду с разрешением 176×144 пикселей;

– CIF (Common Intermediate Format) – это видеоформат, используемый в системах видеоконференц-связи, который выдает видеопоток в тридцать кадров в секунду с разрешением 352×288 пикселей;

– I (Advanced Intra Coding mode) – режим улучшенного Intra-кодирования (термин Intra-кодирование означает, что различные техники сжатия с потерями и без потерь применяются только к текущему кадру, причем не принимается во внимание связь текущего кадра с другим любым кадром в видеопоследовательности). Этот режим увеличивает эффективность сжатия I-кадров и P-кадров с большим содержанием intra-закодированных блоков.

```

Frame 15 (1251 bytes on wire, 1251 bytes captured)
Ethernet II, Src: wistron_98:a9:e5 (00:1f:16:98:a9:e5), Dst: CompalCo_f0:37:70 (00:16:d4:f0:37:70)
Internet Protocol, Src: 192.168.0.100 (192.168.0.100), Dst: 192.168.0.5 (192.168.0.5)
User Datagram Protocol, Src Port: 18900 (18900), Dst Port: sip (5060)
Session Initiation Protocol
Request-Line: INVITE sip:200@192.168.0.5 SIP/2.0
Message Header
Via: SIP/2.0/UDP 192.168.0.100:18900;branch=z9hG4bk-d8754z-e27a6a77885bc046-1---d8754z-;rport
Max-Forwards: 70
Contact: <sip:100@192.168.0.100:18900>
To: "200"<sip:200@192.168.0.5>;tag=3f37532e
From: "Abonent A"<sip:100@192.168.0.5>;tag=857dc618
Call-ID: ZbjMTg2ODlhYzk3YzkwMjY2MDFmYmIwOWUyMGQzZTk.
CSeq: 3 INVITE
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, NOTIFY, MESSAGE, SUBSCRIBE, INFO
Content-Type: application/sdp
Proxy-Authorization: Digest username="Abonent A",realm="sipnet.by",
nonce="47816bab45ea7c3402ed79617c384686",uri="sip:200@192.168.0.5",response="f9a77c6def4172db16cb64b9194bca02"
User-Agent: X-Lite release 1104o stamp 56125
Content-Length: 475
Message Body
Session Description Protocol
Session Description Protocol Version (v): 0
Owner/Creator, Session Id (o): - 1 3 IN IP4 192.168.0.100
Session Name (s): CounterPath X-Lite 3.0
Connection Information (c): IN IP4 192.168.0.100
Time Description, active time (t): 0 0
Media Description, name and address (m): audio 41114 RTP/AVP 107 0 8 101
Media Attribute (a): alt:1 1 : 7ByLgwoC MrhDLZkQ 192.168.0.100 41114
Media Attribute (a): ftmp:101 0-15
Media Attribute (a): rtpmap:107 BV32/16000
Media Attribute (a): rtpmap:101 telephone-event/8000
Media Attribute (a): sendrecv
Media Description, name and address (m): video 37610 RTP/AVP 115 34
Media Type: video
Media Port: 37610
Media Proto: RTP/AVP
Media Format: 115
Media Format: ITU-T H.263
Media Attribute (a): alt:1 1 : SasnIc0y 0iPMV3vI 192.168.0.100 37610
Media Attribute Fieldname: alt
Media Attribute value: 1 1 : SasnIc0y 0iPMV3vI 192.168.0.100 37610
Media Attribute (a): ftmp:115 QCIF=1;CIF=1;I=1;J=1;T=1
Media Attribute Fieldname: ftmp
Media Format: 115 [telephone-event]
Media format specific parameters: QCIF=1
Media format specific parameters: CIF=1
Media format specific parameters: I=1
Media format specific parameters: J=1
Media format specific parameters: T=1
Media Attribute (a): ftmp:34 QCIF=1;CIF=1
Media Attribute Fieldname: ftmp
Media Format: 34 [telephone-event]
Media format specific parameters: QCIF=1
Media format specific parameters: CIF=1
Media Attribute (a): rtpmap:115 H263-1998/90000
Media Attribute Fieldname: rtpmap
Media Format: 115
MIME Type: H263-1998
Media Attribute (a): rtpmap:34 H263/90000
Media Attribute Fieldname: rtpmap
Media Format: 34
MIME Type: H263
Media Attribute (a): sendrecv

```

Рис. 20. Модифицированный запрос INVITE

Увеличение производительности достигается за счет пространственного предсказания DCT-коэффициентов intra-закодированных блоков;

– J (Deblocking Filter mode) – режим фильтра устранения блочности. Этот адаптивный фильтр используется внутри петли кодирования, чтобы уменьшить количество артефактов блочности в декодированном видеоизображении путем фильтрации границ блоков. Часто это увеличивает качество воспроизведения видео;

– T (Modified Quantization mode) – режим модифицированного квантования. Позволяет кодеру выбирать одну из нескольких таблиц квантования при обработке каждого макроблока. Этот режим может увеличивать эффективность кодирования, уменьшая артефакты цветности путем сокращения размера шага квантования хроматических компонент видеосигнала.

Поле Media Attribute (a): fmtp:34 уточняет формат 34. Этот формат поддерживает описанные выше форматы QCIF и CIF.

Поле Media Attribute (a): rtpmap:115 уточняет формат трафика номер 115. Его содержание означает, что должен быть использован кодек H.263 версии 1998 года с частотой дискретизации 90 кГц.

Поле Media Attribute (a): rtpmap:34 уточняет формат трафика номер 34. Его содержание означает, что должен быть использован кодек H.263 с частотой дискретизации 90 кГц.

Поле Media Attribute (a): sendrecv означает, что клиент должен быть запущен в режиме приема и передачи. Это необходимо для интерактивных конференций с клиентами, которые по умолчанию находятся только в принимающем режиме.

После принятия модифицированного запроса INVITE прокси-сервер посылает абоненту А ответ 100 Trying, затем пересылает модифицированный запрос INVITE вызываемому абоненту. Последний после обработки запроса направляет в сторону сервера ответ 200 ОК, сервер подтверждает прием сигналом АСК. Прокси-сервер посылает вызываемому абоненту ответ 200 ОК, прием которого тот подтверждает сообщением АСК.

Если сравнить процесс модификации сессии с процессом установления соединения, то можно сделать вывод, что первый происходит по тому же алгоритму, что и второй, за исключением отсутствия сигнала контроля посылки вызова – 180 Ringing.

Разрыв соединения может инициироваться любым из абонентов путем посылки запроса BYE. Пусть инициатива исходит от пользователя А. На рис. 21 изображено соответствующее сообщение BYE.

Запрос BYE содержит стандартные поля протокола SIP, такие, как Request-Line, Via, Contact, To, From, Call-ID, Cseq, Proxy-Authorization.

Поле Reason содержит указание причины, по которой текущий сеанс связи был прерван. Стока SIP;description="User Hung Up" означает, что причина разрыва указана в формате протокола SIP (в отличие от формата,

соответствующего рекомендации ITU-T Q.850) и пользователь на другом конце повесил трубку. Запрос BYE не содержит тела сообщения.

В ответ на запрос BYE прокси-сервер посылает сообщение 200 ОК, которое не содержит тела сообщения. Прокси-сервер направляет запрос BYE другой стороне.

После получения ответа 200 ОК сессия считается завершенной.

```

+ Frame 23 (694 bytes on wire, 694 bytes captured)
+ Ethernet II, Src: wistron_98:a9:e5 (00:1f:16:98:a9:e5), Dst: CompalCo_f0:37:70 (00:16:d4:f0:37:70)
+ Internet Protocol, Src: 192.168.0.100 (192.168.0.100), Dst: 192.168.0.5 (192.168.0.5)
+ User Datagram Protocol, Src Port: 18900 (18900), Dst Port: sip (5060)
+ Session Initiation Protocol
  + Request-Line: BYE sip:200@192.168.0.5 SIP/2.0
    Method: BYE
    [Resent Packet: False]
  + Message Header
    + Via: SIP/2.0/UDP 192.168.0.100:18900;branch=z9hG4bK-d8754z-7b21ee0b3d163924-1---d8754z-;rport
      Max-Forwards: 70
    + Contact: <sip:100@192.168.0.100:18900>
    + To: "200"<sip:200@192.168.0.5>;tag=3f37532e
    + From: "Abonent A"<sip:100@192.168.0.5>;tag=857dc618
      Call-ID: zjBjMTg2oDlhYzk3YzkwMjY2MDFmYmIwOWUyMGZzZTk.
    + CSeq: 4 BYE
    + Proxy-Authorization: Digest username="Abonent A",realm="sipnet.by",
      nonce="47816bab45ea7c3402ed79617c384686",uri="sip:200@192.168.0.5",response="a8b237fb2a34fe90957e92d7c15f3957"
    User-Agent: X-Lite release 1104o stamp 56125
    + Reason: SIP;description="user Hung Up"
      Content-Length: 0
  
```

Рис. 21. Сообщение BYE

Протокол SIP поддерживает передачу мгновенных сообщений. IM (instant messages) – это обмен сообщениями между набором участников, близкий к обмену в реальном времени.

No. -	Time	Source	Destination	Protocol	Info
2	16.596569	192.168.0.100	192.168.0.5	SIP	Request: MESSAGE sip:200@192.168.0.5
3	16.596817	192.168.0.5	192.168.0.100	SIP	Status: 407 Proxy Authentication Required
4	16.699133	192.168.0.100	192.168.0.5	SIP	Request: MESSAGE sip:200@192.168.0.5
5	16.699385	192.168.0.5	192.168.0.100	SIP	Status: 200 OK
8	36.416339	192.168.0.100	192.168.0.5	SIP	Request: MESSAGE sip:200@192.168.0.5 (text/html)
9	36.416632	192.168.0.5	192.168.0.200	SIP	Request: MESSAGE sip:200@192.168.0.200:46674 (text/html)
10	36.416725	192.168.0.5	192.168.0.100	SIP	Status: 200 OK
11	36.522365	192.168.0.200	192.168.0.5	SIP	Status: 200 OK
12	43.826967	192.168.0.200	192.168.0.5	SIP	Request: MESSAGE sip:100@192.168.0.5
13	43.827224	192.168.0.5	192.168.0.200	SIP	Status: 200 OK
15	53.636205	192.168.0.200	192.168.0.5	SIP	Request: MESSAGE sip:100@192.168.0.5 (text/html)
16	53.636475	192.168.0.5	192.168.0.100	SIP	Request: MESSAGE sip:100@192.168.0.100:65496 (text/html)
17	53.636566	192.168.0.5	192.168.0.200	SIP	Status: 200 OK
18	53.738828	192.168.0.100	192.168.0.5	SIP	Status: 200 OK

Рис. 22. Процесс обмена мгновенными сообщениями

Обычно содержание сообщений составляют короткие текстовые послания. Как правило, эти послания не сохраняются, однако такая возможность не исключается. Мгновенные сообщения отличаются от

электронной почты тем, что IM обычно группируются вокруг коротких сеансов взаимодействия, которые состоят из ряда небольших сообщений, посылаемых в обе стороны.

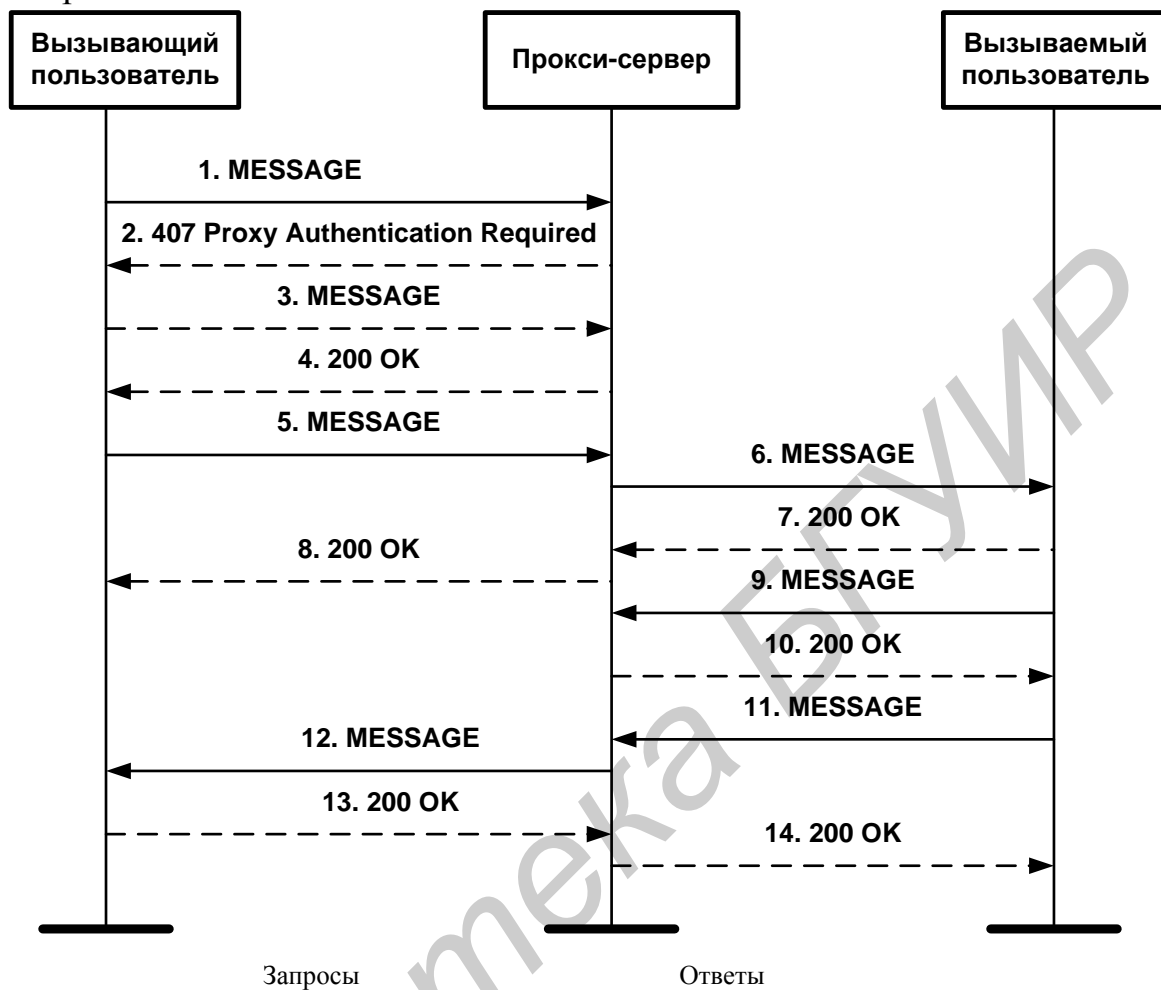


Рис. 23. Структура обмена мгновенными сообщениями

В протоколе SIP запрос типа MESSAGE предназначен для передачи мгновенных текстовых сообщений с использованием модели, похожей на модель функционирования двустороннего пейджера или работу телефона при отправке SMS. При этом не существует прямой связи между сообщениями и каждое текущее сообщение независимо от другого, а информация о том, что осуществляется взаимодействие, отражается только в пользовательском интерфейсе клиента. Такой подход отличается от сессионной модели, в которой происходит однозначное взаимодействие участников с чётко определённым началом и концом сессии.

Процесс обмена мгновенными сообщениями между пользователем А и пользователем в контекстном окне анализатора трафика приведен на рис. 22, а структура обмена мгновенными сообщениями представлена на рис. 23. После первой попытки послать сообщение пользователь А получает запрос аутентификации.

Далее все его сообщения содержат информацию для аутентификации.



```

⊞ Frame 4 (996 bytes on wire, 996 bytes captured)
⊞ Ethernet II, Src: Wistron_98:a9:e5 (00:1f:16:98:a9:e5), Dst: CompalCo_f0:37:70 (00:16:d4:f0:37:70)
⊞ Internet Protocol, Src: 192.168.0.100 (192.168.0.100), Dst: 192.168.0.5 (192.168.0.5)
⊞ User Datagram Protocol, Src Port: 65496 (65496), Dst Port: sip (5060)
⊞ Session Initiation Protocol
  ⊞ Request-Line: MESSAGE sip:200@192.168.0.5 SIP/2.0
    Method: MESSAGE
    [Resent Packet: False]
  ⊞ Message Header
    ⊞ Via: SIP/2.0/UDP 192.168.0.100:65496;branch=z9hG4bK-d8754z-1f35ee0b2d7ec05d-1---d8754z-;rport
      Max-Forwards: 70
    ⊞ To: "200"<sip:200@192.168.0.5>
    ⊞ From: "Abonent A"<sip:100@192.168.0.5>;tag=23440e42
      Call-ID: NDg2MmNmMDI1ODVkwZlM2ViNDcxYzhkYmY1YzkxYWU.
    ⊞ CSeq: 3 MESSAGE
      Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, NOTIFY, MESSAGE, SUBSCRIBE, INFO
      Content-Type: application/im-iscomposing+xml
    ⊞ Proxy-Authorization: Digest username="100",realm="sipnet.by",nonce="600c72fd78a348845b6271f8188121b4",uri="sip:200@192.168.0.5",
      User-Agent: X-Lite release 1103k stamp 53621
      Content-Length: 262
  ⊞ Message Body
    <?xml version='1.0' encoding='UTF-8'?>\n
    <isComposing xmlns='urn:ietf:params:xml:ns:im-iscomposing'\n
      xmlns:xsi='http://www.w3.org/2001/XMLSchema-instance'>\n
      <state>active</state>\n
      <contenttype>text/html</contenttype>\n
      <refresh>60</refresh>\n
    </isComposing>

```

Рис. 24. Первый запрос MESSAGE

```

⊞ Frame 8 (828 bytes on wire, 828 bytes captured)
⊞ Ethernet II, Src: Wistron_98:a9:e5 (00:1f:16:98:a9:e5), Dst: CompalCo_f0:37:70 (00:16:d4:f0:37:70)
⊞ Internet Protocol, Src: 192.168.0.100 (192.168.0.100), Dst: 192.168.0.5 (192.168.0.5)
⊞ User Datagram Protocol, Src Port: 65496 (65496), Dst Port: sip (5060)
⊞ Session Initiation Protocol
  ⊞ Request-Line: MESSAGE sip:200@192.168.0.5 SIP/2.0
    Method: MESSAGE
    [Resent Packet: False]
  ⊞ Message Header
    ⊞ Via: SIP/2.0/UDP 192.168.0.100:65496;branch=z9hG4bK-d8754z-252cfc449e42401b-1---d8754z-;rport
      Max-Forwards: 70
    ⊞ To: "200"<sip:200@192.168.0.5>
    ⊞ From: "Abonent A"<sip:100@192.168.0.5>;tag=23440e42
      Call-ID: NDg2MmNmMDI1ODVkwZlM2ViNDcxYzhkYmY1YzkxYWU.
    ⊞ CSeq: 4 MESSAGE
      Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, NOTIFY, MESSAGE, SUBSCRIBE, INFO
      Content-Type: text/html
    ⊞ Proxy-Authorization: Digest username="100",realm="sipnet.by",nonce="600c72fd78a348845b6271f8188121b4",uri="sip:200@192.168.0.5"
      User-Agent: X-Lite release 1103k stamp 53621
      Content-Length: 115
  ⊞ Message Body
    ⊞ Line-based text data: text/html
      [truncated] <SPAN STYLE="FONT-FAMILY:Arial; FONT-SIZE:12pt ">\320\237\321\200\320\270\320\262\320\265\321\202! \320\255\321\2

```

Рис. 25. Запрос MESSAGE с пользовательской информацией

На каждый запрос MESSAGE приходит ответ 200 OK. Когда получен ответ 200 OK, это означает, что сообщение успешно доставлено адресату, но не

говорит о том, что адресат прочитал сообщение. В первом запросе MESSAGE клиент в формате языка XML информирует прокси-сервер о том, в каком виде он будет передавать сообщения другому абоненту. Так, в примере запроса, изображенном на рис. 24, сообщается, что пользовательская информация будет передаваться в формате text/html, а на рис. 25 представлен запрос MESSAGE, который переносит в теле сообщения пользовательское сообщение в формате text/html.

Ответы 200 OK на запросы MESSAGE не содержат тела сообщения, но содержат стандартные поля протокола SIP, такие, как Request-URI, Via, To, From, Cseq, Call-ID.

Библиотека БГУИР

## Контрольные вопросы

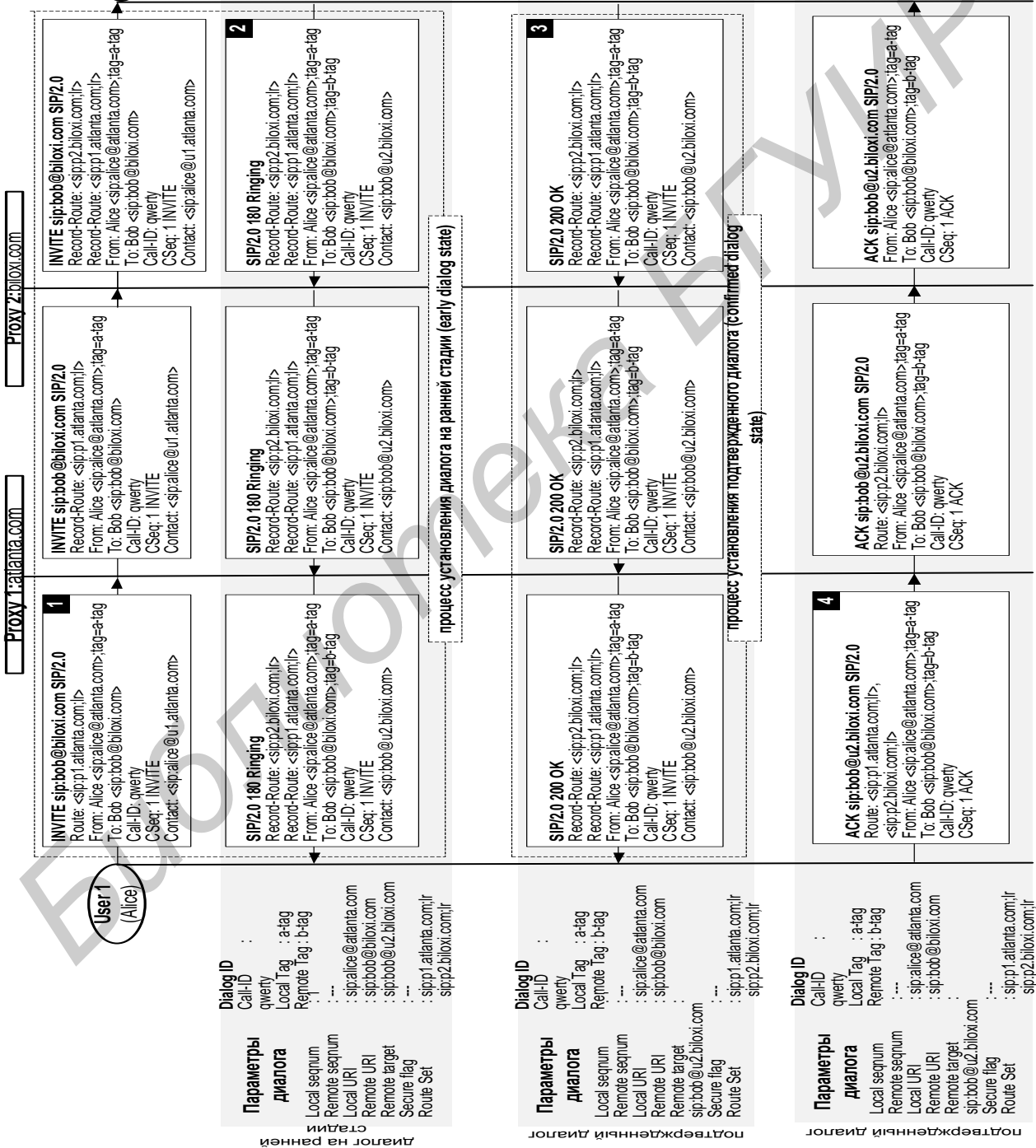
1. Пояснить типы адресации, применяемые при установлении мультимедийных приложений на основе протокола SIP.
2. Пояснить назначение и формат заголовков маршрутной информации и структуру клиентской информации в теле сообщений SIP.
3. Пояснить принципы выполнения «роуминга» на сети SIP.
4. Пояснить структуру диалога при выполнении процедуры регистрации.
5. Перечень процедур и структура диалога при установлении соединения на основе протокола SIP.
6. Перечень процедур и структура диалога при разрушении соединения на основе протокола SIP.
7. Пояснить параметры диалога при выполнении процедур мультимедийной сессии, лексическая структура SIP-сообщений которой приведена в приложении.
8. В какие моменты времени терминалы пользователей посылают информацию о своих функциональных возможностях? В каких сообщениях эта информация располагается?
9. Какое минимальное число сообщений необходимо для установления соединения?
10. Пояснить формат тела сообщений SIP при установлении видеотелефонного соединения.
11. Функциональные возможности и характеристики минисервера MMS, терминала X-Lite и анализатора трафика Wireshark.
12. Пояснить последовательность настроек минисервера MMS, терминала X-Lite и анализатора трафика Wireshark.
13. Возможности анализа характеристик пакетного трафика на основе анализатора Wireshark.
14. Возможности абонентского сервиса на основе программных SIP-терминалов X-Lite?
15. Возможности сетевого сервиса на основе минисервера MMS.

## Литература

1. MiniSipServer manual [Электронный ресурс] / MyVoipApp Support Team. – Электронные данные. – Режим доступа: [http://www.myvoipapp.com/docs/mss\\_services/manual/index.html](http://www.myvoipapp.com/docs/mss_services/manual/index.html). – Дата доступа: 2010 г.
2. X-Lite 3.0 User Guide [Электронный ресурс] / CounterPath Solutions, Inc. – Электронные данные. – Режим доступа: X-Lite3.0\_UserGuide.pdf. – Дата доступа: 2010 г.
3. Малых, Н. Анализатор протоколов Ethereal [Электронный ресурс] / Н. Малых. – Электронные данные. – Режим доступа: Wireshark.pdf. – Дата доступа: 2010 г.
4. Хоменок, М. Ю. Методическое пособие «Сигнализация на сетях передачи данных с пакетной коммутацией. Протокол SIP» М. Ю. Хоменок. – Минск : БГУИР, 2011.
5. Гольдштейн, Б. С. Протокол SIP. Справочник / Б. С. Гольдштейн, А. А. Зарубин, В. В. Саморезов. – СПб. : БХВ – Санкт-Петербург, 2005.
6. RFC 3261 SIP: Session Initiation Protocol [Электронный ресурс] / J. Rosenberg, H. Schulzrinne, G. Camarillo. – Электронные данные. – Режим доступа: <http://tools.ietf.org/html/rfc3261>. – Дата доступа: 2010 г.
7. ETSI TS 102 027-2 V4.1.1 (2006-07). Технические спецификации.

ПРИЛОЖЕНИЕ 1:

Лексическая структура SIP-сообщений в фазе установления сессии



диалог на ранней стадии

<b>Dialog ID</b>	Call-ID : query
<b>Параметры диалога</b>	Local Tag : b-tag
	Remote Tag : a-tag
	Local sequum : sip:bob@biloxi.com
	Remote sequum : sip:alice@atlanta.com
	Local URI : sip:alice@atlanta.com
	Remote URI : sip:alice@u1.atlanta.cc
	Secure flag : ...
	Route Set : sip:p2.biloxi.com;lr sip:p1.atlanta.com;lr

подтвержденный диалог

<b>Dialog ID</b>	Call-ID : query
<b>Параметры диалога</b>	Local Tag : b-tag
	Remote Tag : a-tag
	Local sequum : sip:bob@biloxi.com
	Remote sequum : sip:alice@atlanta.com
	Local URI : sip:alice@atlanta.com
	Remote URI : sip:alice@u1.atlanta.cc
	Secure flag : ...
	Route Set : sip:p2.biloxi.com;lr sip:p1.atlanta.com;lr

подтвержденный диалог

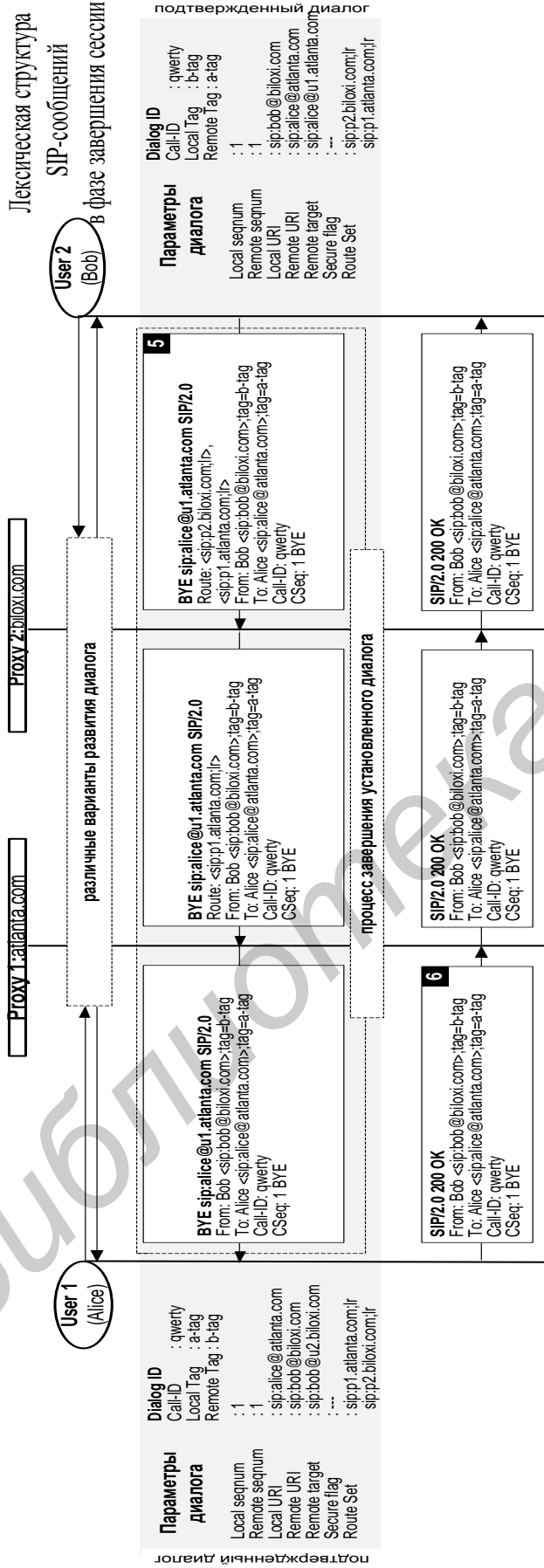
<b>Dialog ID</b>	Call-ID : query
<b>Параметры диалога</b>	Local Tag : b-tag
	Remote Tag : a-tag
	Local sequum : sip:bob@biloxi.com
	Remote sequum : sip:alice@atlanta.com
	Local URI : sip:alice@atlanta.com
	Remote URI : sip:alice@u1.atlanta.cc
	Secure flag : ...
	Route Set : sip:p2.biloxi.com;lr sip:p1.atlanta.com;lr

ПРИЛОЖЕНИЕ 2:

Лексическая структура

SIP-сообщений

В фазе завершения сессии



Библиотека БГУИР

*Учебное издание*

**Хоменок Михаил Юлианович**

**СТРУКТУРА СООБЩЕНИЙ  
ПРОТОКОЛА SIP**

Методическое пособие  
к лабораторно-практическим занятиям по курсу  
«Сетевые технологии и сигнализация в телекоммуникациях»  
для студентов специальностей  
1-45 01 03 «Сети телекоммуникаций»,  
1-45 01 05 «Системы распределения мультимедийной информации»  
всех форм обучения

Редактор Т. П. Андрейченко  
Корректор И. П. Острикова

---

Подписано в печать 01.09.2011.  
Гарнитура «Гаймс».  
Уч. изд. л. 1,5.

Формат 60×84 1/16.  
Отпечатано на ризографе.  
Тираж 50 экз.

Бумага офсетная.  
Усл. печ. л. 1,98.  
Заказ 289.

---

Издатель и полиграфическое исполнение: учреждение образования  
«Белорусский государственный университет информатики и радиоэлектроники»  
ЛИ №02330/0494371 от 16.03.2009, ЛП №02330/0494175 от 03.04.2009.  
220013, Минск, П. Бровки, 6

Библиотека БГУИР