

Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное
учреждение высшего профессионального образования
«Севастопольский государственный университет»

**ИССЛЕДОВАНИЕ СПОСОБОВ КОНФИГУРАЦИИ
СЕТЕВЫХ СЕРВЕРНЫХ СЛУЖБ СТЕКА
ПРОТОКОЛОВ ТСР/ПР**

Методические указания

к выполнению лабораторной работы по дисциплине
«Инфокоммуникационные системы и сети»

Для студентов, обучающихся по направлению 09.03.02
«Информационные системы и технологии»
и 09.03.03 «Прикладная информатика»
по учебному плану подготовки бакалавров
дневной и заочной форм обучения

**Севастополь
2020**

Исследование способов конфигурации сетевых серверных служб стека протоколов TCP/IP. Методические указания к лабораторным занятиям по дисциплине «Инфокоммуникационные системы и сети» / Сост. В.С. Чернега, – Севастополь: Изд-во СевГУ, 2020 – 12 с.

Методические указания предназначены для проведения лабораторных работ по дисциплине «Инфокоммуникационные системы и сети». Целью методических указаний является помочь студентам в изучении и исследовании протоколов прикладного уровня и способов конфигурации HTTP-, DNS- и DHCP-серверов. Излагаются теоретические и практические сведения необходимые для выполнения лабораторной работы, требования к содержанию отчета.

Методические указания рассмотрены и утверждены на методическом семинаре и заседании кафедры информационных систем
(протокол № от 2020 г.)

Рецензент: Кротов К.В., канд. техн. наук, доцент кафедры ИС

1 Цель работы

Исследование особенностей использования основных сетевых серверных служб стека протоколов TCP/IP и конфигурации серверов, реализующих эти службы, приобрести практические навыки по конфигурации серверного сетевого оборудования.

2 Краткие теоретические сведения

В простейшем понимании служба — это пара программ, взаимодействующих между собой согласно определенным протоколами по схеме клиент-сервер. Одна из программ этой пары называется сервером, а другая — клиентом. Соответственно, когда говорят о работе сетевых служб, речь идет о взаимодействии оборудования и программного обеспечения сервера с оборудованием и программным обеспечением клиента, обеспечивающих функционирование компьютерной сети.

Протоколы, реализующие сетевые службы, относятся к протоколам прикладного уровня. Существует большое количество протоколов этого уровня и выполняют они совершенно различные функции. К наиболее часто используемым протоколам прикладного уровня относятся протоколы HTTP, DNS, DHCP, SMTP и POP3, Telnet, SSH, FTP и TFTP.

В данной работе исследуются протоколы, предназначенные для облегчения администрирования компьютерных сетей, в частности: HTTP, DNS и DHCP.

1) **Протокол передачи гипертекста HTTP** (*HyperText Transport Protocol*), используемый обычно для получения информации с веб-сайтов. Построен на основе клиент-серверной модели, то есть существуют клиенты, формирующие и отправляющие запрос и серверы, которые принимают запросы и, соответственно, на них отвечают. Передача данных по протоколу HTTP обычно происходит через TCP/IP-соединения. Серверное программное обеспечение при этом использует TCP-порт 80 (и, если порт не указан явно, то обычно клиентское программное обеспечение по умолчанию использует именно 80-й порт для открываемых HTTP-соединений), хотя может использовать и любой другой.

В качестве клиентов выступают веб-браузеры: Internet Explorer, Mozilla Firefox, Google Chrome и т.д, а в качестве серверного ПО используются серверы Apache, IIS (*Internet Information Server*), nginx (engine x) и др.

Кроме протокола HTTP имеется расширенная версия HTTPS, согласно которой все данные передаются в зашифрованном виде.

2) **Протокол разрешения доменных имен DNS** (*Domain Name System*) относится к прикладному уровню эталонной модели. При этом используется 53-й TCP- или UDP-порт. Чаще всего применяется для получения IP-адреса по имени хоста (компьютера или устройства). Имеется распределённая база данных DNS, которая поддерживается с помощью иерархии DNS-серверов, взаимодействующих по DNS-протоколу.

3) **Протокол DHCP** (*Dynamic Host Configuration Protocol*) — это одна из служб поддержки протокола TCP/IP, разработанная для упрощения админи-

стрирования IP-сети за счет использования специально настроенного сервера для централизованного управления IP-адресами и другими параметрами протокола TCP/IP, необходимыми сетевым узлам. Сервер DHCP избавляет сетевого администратора от необходимости ручного выполнения операций. С его помощью реализуется:

- автоматическое назначение сетевым узлам IP-адресов и прочих параметров протокола TCP/IP (например, маска подсети, адрес основного шлюза подсети, адреса серверов DNS и WINS);
- защита от дублирования IP-адресов, назначаемых различным узлам сети;
- освобождение IP-адресов узлов, удаленных из сети;
- ведение централизованной БД выданных IP-адресов.

При загрузке компьютера, настроенного на автоматическое получение IP-адреса, или при смене статической настройки IP-конфигурации на динамическую, а также при обновлении IP-конфигурации сетевого узла происходят следующие действия:

- 1) компьютер посылает широковещательный запрос на обнаружение доступного DHCP-сервера, (DHCP Discover);
- 2) DHCP-серверы, получившие данный запрос, посылают данному сетевому узлу свои предложения IP-адреса (DHCP Offer);
- 3) клиент отвечает на предложение, полученное первым, соответствующему серверу запросом на выбор арендуйемого IP-адреса (DHCP Request);
- 4) DHCP-сервер регистрирует в своей БД выданную IP-конфигурацию (вместе с именем компьютера и физическим адресом его сетевого адаптера) и посыпает клиенту подтверждение на аренду IP-адреса (DHCP Acknowledgement).

При планировании серверов DHCP:

- желательно в каждой IP-сети установить отдельный DHCP-сервер;
- если нет возможности установить свой сервер в каждой IP-сети, необходимо на маршрутизаторах, объединяющих IP-сети, запустить и настроить агент ретрансляции DHCP-запросов (*DHCP Relay Agent*) таким образом, чтобы он пересыпал широковещательные запросы DHCP из подсети, в которой нет DHCP-сервера, на соответствующий DHCP-сервер, а на самом DHCP-сервере создать области для всех обслуживаемых IP-сетей;

• для повышения отказоустойчивости следует установить несколько серверов DHCP, при этом на каждом DHCP-сервере, кроме областей для "своих" IP-сетей, необходимо создать области для других подсетей (при этом диапазоны IP-адресов в таких резервных областях не должны пересекаться с основными областями, созданными на серверах DHCP в "своих" подсетях);

• в больших IP-сетях DHCP-серверы должны иметь мощные процессоры, достаточно большие объемы оперативной памяти и быстродействующие дисковые подсистемы, т.к. обслуживание большого количества клиентов требует интенсивной работы с базой данных DHCP-сервера.

3 Описание лабораторной установки

В качестве лабораторной установки используется персональный компьютер с инсталлированной программой Packet Tracer, позволяющей осуществлять моделирования компьютерных сетей, построенных на оборудовании корпорации Cisco. Подробно описание пакета моделирования и работы с ним приведено в лабораторной работе №1. В программе имеется возможность включать в состав моделируемых сетей серверы практически всех типов и осуществлять их конфигурацию. К наиболее широко используемыми серверами, моделируемыми системой Packet Tracer, относятся следующие типы серверов.

Cisco HTTP (WEB) сервер – позволяет создавать простейшие веб-странички и проверять прохождение пакетов на 80-ый порт сервера. Эти серверы предоставляют доступ к веб-страницам и сопутствующим ресурсам, например, изображением.

DHCP сервер – позволяет организовывать пулы сетевых настроек для автоматического конфигурирования сетевых интерфейсов. *Dynamic Host Configuration Protocol* обеспечивает автоматическое распределение IP-адресов между компьютерами в сети. Такая технология широко применяется в локальных сетях с общим выходом в *Интернет*.

DNS сервер – позволяет организовать службу разрешения доменных имён. Функция DNS-сервера заключается в преобразовании доменных имен серверов в IP-адреса.

Cisco EMAIL – почтовый сервер, для проверки почтовых правил. Электронное письмо нельзя послать непосредственно получателю – сначала оно попадает на сервер, на котором зарегистрирована учетная запись отправителя. Тот, в свою очередь, отправляет "посылку" серверу получателя, с которого последний и забирает сообщение.

FTP – файловый сервер. В его задачи входит хранение файлов и обеспечение доступа к ним клиентских ПК, например, по протоколу *FTP*. Ресурсы файла-сервера могут быть либо открыты для всех компьютеров в сети, либо защищены системой идентификации и правами доступа.

AAA – сервер авторизации.

В настоящей работе будут исследоваться процессы конфигурации Web-, DHCP- и DNS-серверов.

4 Программа выполнения работы

4.1 Повторить теоретический материал по иерархии протоколов стека TCP/IP, по протоколам прикладного уровня и составу полей кадров и пакетов этих протоколов (выполняется в процессе домашней подготовки).

4.2 Составить в рабочем окне эмулятора схему исследуемой сети, изображенной на рисунке 4.1.

4.3 Установить для всех серверов сети статический режим адресации и задать их адреса в следующем виде: XY.0.0.10 – DHCP-сервер; XY.0.0.100 –

DNS-сервер; XY.0.0.100 – HTTP-сервер www.sevgu.ru; XY.0.0.200 – HTTP-сервер www.kaf.is. Здесь X-предпоследняя цифра зачетной книжки, а Y-предпоследняя.

4.4 Задать режим динамической адресации для оконечных устройств сети, и провести установку и настройку DHCP-сервера на компьютере XY.0.0.10.

4.5 Установить на серверный компьютер XY.0.0.100 DNS-сервер и осуществить его настройку.

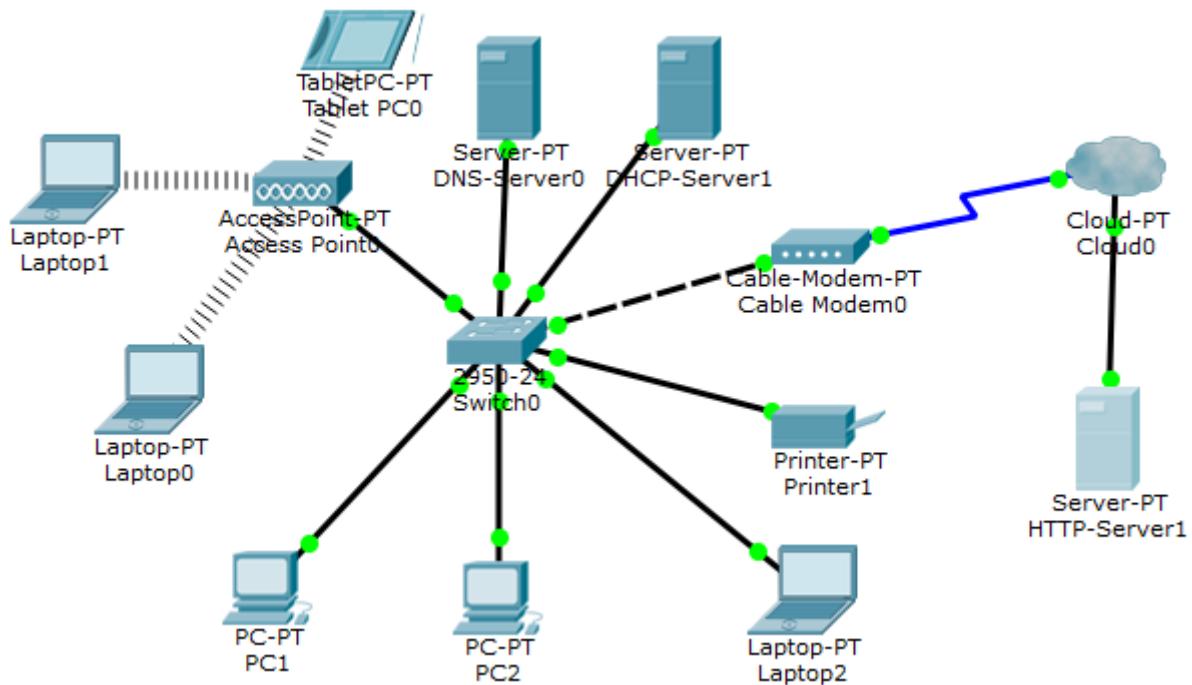


Рисунок 4.1 – Схема исследуемой сети с сетевыми службами

4.6 Установить на серверный компьютер XY.0.0.100 HTTP-сервер, и разместить на нем страничку сайта www.sevgu.ru с информацией о университете.

4.7 Установить на серверный компьютер XY.0.0.200 HTTP-сервер, и разместить на нем страничку сайта www.kaf.is.ru с рекламной информацией о кафедре ИС.

4.8 Провести проверку связи оконечных устройств друг с другом и доступа к страницам сайтов по их IP-адресам и по доменным символьическим именам в реальном режиме и режиме симуляции.

4.9 Исследовать структуру пакетов при обращении к странице одного из сайтов.

4.1 Оформить отчет и сделать выводы по работе.

5 Методические рекомендации по выполнению лабораторной работы

5.1 Подключение удаленного сервера через облако Интернета

Связь коммутатора с облачным устройством осуществляется с помощью коаксиального кабеля и кабельного модема. Чтобы пакеты могли передаваться через облако нужно настроить порты со стороны модема и удаленного сервера. Для этого нужно выполнить следующие действия.

Щелкните пиктограмму облака Интернета в логическом рабочем пространстве Packet Tracer и выберите вкладку Physical (Физические). Для облачного устройства потребуются два модуля, если они еще не установлены. Модуль PT-CLOUD-NM-1CX необходим для подключения службы кабельного модема, а модуль PT-CLOUD-NM-1CFE — для подключения медного кабеля Ethernet. Если эти модули отсутствуют, отключите физические облачные устройства, нажав кнопку питания, и перетащите оба этих модуля в пустые порты для модулей устройства. После этого снова включите питание.

Находясь на вкладке **Config** (Конфигурация), выберите Ethernet в разделе **INTERFACE** (Интерфейс) в левой панели. В окне конфигурации Ethernet выберите **Cable** (Кабель) в поле Provider Network.

Для определения выходного и входного портов облачного пространства откройте вкладку **Config** в окне Cloud device. В левой панели выберите **Cable** в разделе **CONNECTIONS** (Подключения). В первом раскрывающемся списке выберите пункт Coaxial (Коаксиальный), а во втором — Ethernet. Затем нажмите кнопку **Add** (Добавить), чтобы добавить их в качестве выходного и входного портов.

5.2 Создание служб и конфигурация серверов

Для установки любой службы на серверном компьютере щелкните левой кнопкой мыши по компьютеру и выберите вкладку **Services** (Службы).

При установке службы DHCP Выберите **DHCP** в списке **SERVICES** в панели слева. В окне конфигурации DHCP настройте следующие параметры DHCP:

- нажмите **On**, чтобы включить службу DCHP;
- задайте имя пула адресов Pool name, например DHCPpool;
- задайте адреса: Шлюза по умолчанию, DNS-сервера, Начальный IP-адрес, Маску подсети и Максимальное число пользователей в сети;
- Нажмите **Add**, чтобы добавить пул.

Для установки и конфигурации DNS-сервера необходимо активировать Server0 и открыть закладку Services, на которой выбрать службу DNS. В рабочем окне нужно задать две ресурсные записи (Resource Records) в прямой зоне DNS, которая представляет собой часть дерева доменных имен (включая ресурсные записи), размещаемая как единое целое на сервере доменных имен (DNS-сервере). Сначала в ресурсной записи типа A Record необходимо связать

доменное имя компьютера с его IP-адресом. Для этого в окошке Name задать имя DNS -сервера (например, server0.mail.ru), а в окошке Address занести его IP-адрес (например, 10.0.0.100). Затем в окошке Type следует выбрать тип записи «A Record» и нажать на кнопку Add, а также активировать переключатель On.

Далее в окошко Name внести имя сайта (например, www.mail.ru), а в окошко Host Name – имя сервера. После этого нужно связать название сайта с сервером, для чего в окошке Type выбрать тип ресурсной записи «CNAME» и нажать кнопку Add (добавить).

Для создания HTTP-сервера необходимо открыть на серверном компьютере вкладку Services, активировать протокол HTTP и выбрать режим редактирования (edit) шаблона страницы сайта с названием **index.html**.

В этом окне можно добавить новую страницу или удалить текущую – кнопки + и × соответственно.. Переключение между несколькими страницами осуществляется кнопками < | > .

В окне html кода нужно сформировать текст первой страницы сайта **index.html**. Для этого в рабочем окне нужно ввести следующие директивы:

```
<html>
<body>
<h1>Welcome to WEB-Server</h1>
<p>Server working: <font color="green"><b>OK</b></font></p>
</body>
</html>
```

Текст можно создать в текстовом редакторе и переносить в это окно через буфер обмена. Следует учесть, что текст должен быть только на английском языке!

Примечание: Формат и основные теги языка HTML приведены в приложении А.

5.3 Проверка подключения

Перед началом пингования убедитесь, что ПК получает конфигурационные данные IPv4 от DHCP. Нажмите **PC** в рабочем окне Packet Tracer и выберите вкладку **Desktop**. Щелкните пиктограмму **Command Prompt (Командная строка)**. В командной строке обновите настройки IP-адреса, выполнив команды **ipconfig /release** и **ipconfig /renew**. В выходных данных должно быть указано, что ПК имеет IP-адрес из заданного Вами диапазона, маску подсети, шлюз по умолчанию (при его наличии) и адрес DNS-сервера.

После пингования оконечных устройств по IP-адресам проверьте ответ сервера при запросе на его доменное имя. Для этого в командной строке вы-

полните команду **ping имя сервера**. На получение ответа от команды ping может уйти несколько секунд.

Для проверки работоспособности созданного HTTP сервера нужно открыть окно настройки одного из клиентских компьютеров и на вкладке **Desktop** запустить приложение **Web Browser**. Затем в строке URL задать IP-адрес созданного WEB-сервера и нажать на кнопку **GO**. Появление на экране текстового сообщения, которое было подготовлено на страничке `index.html`, свидетельствует о работоспособности Web-сервера.

Для исследования структуры пакетов при обмене данными между сетевыми устройствами нужно запустить Packet Tracer в режиме симуляции (иконка в правом нижнем углу) и открыть лист событий (нажать Event List). В окне Event List отображаются все пакеты, которые передаются в сети, с указанием источников и получателей пакетов и их типов. При нажатии на цветной квадратик Info исследуемого типа пакета данных (PDU) открывается окно с форматом пакета.

Для более детального анализа содержимого пакета необходимо нажать кнопку Inbound PDU Details (Сведения о входящем PDU) или Outbound PDU Details (Сведения об исходящем PDU).

6 Содержание отчета

- 6.1 Титульный лист.
- 6.2 Схема моделируемой сети.
- 6.3 Скриншоты топологии, реализованных настроек и результатов исследования функционирования сети с пояснениями полученных результатов.
- 6.4 Выводы.

7 Контрольные вопросы

- 7.1 Что представляют собой сетевые службы и зачем они предназначены?
- 7.2 Назовите протоколы прикладного уровня стека TCP/IP и поясните для чего используется тот или иной протокол.
- 7.3 Приведите формат IP-адреса протокола IPv4, назовите его принципиальное отличие от MAC-адреса.
- 7.4 С какой целью разработан протокол ARP и каков основной состав полей заголовка ARP-пакета?
- 7.5 Для чего предназначен протокол DNS и как решается проблема, если в данном DNS-сервере отсутствует запись соответствия символьического и сетевого адресов?
- 7.6 Расскажите об особых (выделенных под специальные нужды) IP-адресах и их назначениях.
- 7.7 Что представляют собой локальные IP-адреса, назовите диапазоны сетей таких адресов. Для чего служит протокол сетевой трансляции адресов?

- 7.8 Опишите формат и использование маски подсети. Как по значению маски определить количество адресов, которое она выделяет? Перечислите известные Вам маски и их характеристики для сети класса С.
- 7.9 Что представляет собой технология бесклассовой междоменной маршрутизации? Запишите адрес и маску суперсети для 2000 хостов.
- 7.10 Для чего предназначен протокол DHCP и может ли компьютерная сеть функционировать без этого протокола?
- 7.11 Что представляет собой маршрут по умолчанию, для чего он используется? Каким образом маршрут по умолчанию указывается в таблице маршрутизации?
- 7.12 Чем отличается статическая маршрутизация от динамической? Приведите названия используемых протоколов динамической маршрутизации.
- 7.13 Какие действия происходят в сети при смене статической адресации на динамическую?
- 7.14 Как рационально спланировать установку DHCP-серверов в локальных и глобальных сетях?
- 7.15 Как на практике в эмуляторе Packet Tracer проверить содержимое заголовков пакетов?

Библиографический список

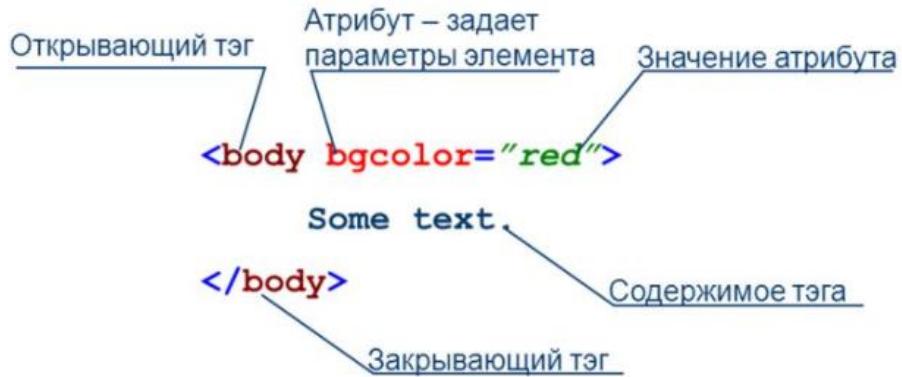
1. Создание простой сети с помощью Packet Tracer.
<https://itmarathon.educom.ru/pdf/admin/%D0%A1%D0%B5%D1%82%D0%B8%D1%82%D1%80%D0%B5%D0%BD%D0%BA%D0%B2.pdf> (дата обращения: 26.07.2020).
2. Дибров М.В. Сети и телекоммуникации. Маршрутизация в IP–сетях. В 2 ч. Часть 2: учебник и практикум для академического бакалавриата / М.В. Дибров. – М.: Изд-во Юрайт, 2019. – 351 с. <https://biblio-online.ru/book/seti-i-telekommunikacii-marshrutizaciya-v-ip-setyah-v-2-ch-chast-2-437865>
3. Сети и телекоммуникации: учебник и практикум для академического бакалавриата / Под ред. К.Е. Самуилова, И.А. Шалимова, Д.С. Кулябова. – М.: Изд-во Юрайт, 2016. – 363 с.
<https://biblio-online.ru/book/seti-i-telekommunikacii-432824>
4. Чернега В.С. Компьютерные сети / В.С. Чернега, Б. Платтнер. — Севастополь: Изд-во СевНТУ, 2006. — 500 с.

Приложение 1. Таблица П1 – Варианты заданий для индивидуального моделирования локальных сетей и серверных служб

Вариант	Пользователи	Сервер HTTP	Сервер DNS	Сервер DHCP
1	2ПК+2ЛТ	Server0	Server1	Server2
2	3ПК+1ЛТ	Server1	Server0	Server0
3	2ПК+3ЛТ	Server2	Server2	Server0
4	4ПК+1ЛТ	Server0	Server0	Server1
5	3ПК+3ЛТ	Server2	Server1	Server1
6	4ПК+2ЛТ	Server1	Server1	Server2
7	3ПК+4ЛТ	Server0	Server0	Server2
8	4ПК+2ЛТ	Server0	Server0	Server1
9	5ПК+1ЛТ	Server2	Server1	Server1
10	5ПК+3ЛТ	Server1	Server1	Server2
11	4ПК+4ЛТ	Server0	Server0	Server2
12	3ПК+5ЛТ	Server0	Server1	Server2
13	4ПК+3ЛТ	Server1	Server0	Server0
14	5ПК+4ЛТ	Server2	Server2	Server0
15	2ПК+5ЛТ	Server0	Server0	Server1
16	3ПК+1ЛТ	Server2	Server1	Server1
17	2ПК+3ЛТ	Server1	Server1	Server2
18	4ПК+1ЛТ	Server0	Server0	Server2
19	3ПК+3ЛТ	Server0	Server0	Server1
20	4ПК+2ЛТ	Server2	Server1	Server1
21	3ПК+4ЛТ	Server1	Server1	Server2
22	5ПК+1ЛТ	Server0	Server0	Server2
23				
24				
25				

ПРИЛОЖЕНИЕ А

Формат и основные теги языка HTML



<html> </html> – HTML-документ

- <head> </head> – информация о документе
 - <title> </title> – название документа
- <body> </body> – тело документа
 - <h1> </h1> – заголовок первого уровня
 - <p> </p> – абзац
 - <a> – гиперссылка
 - – полужирный текст
 - <i> </i> – курсивный текст
 - – изменение шрифта
 - <table> </table> – таблица
 - <tr> </tr> – строка таблицы
 - <td> </td> – ячейка таблицы