



САМАРСКИЙ УНИВЕРСИТЕТ
SAMARA UNIVERSITY

Безопасность веб-приложений

Лекция 1

Александр Сергеев

Кафедра геоинформатики и
информационной безопасности

2022

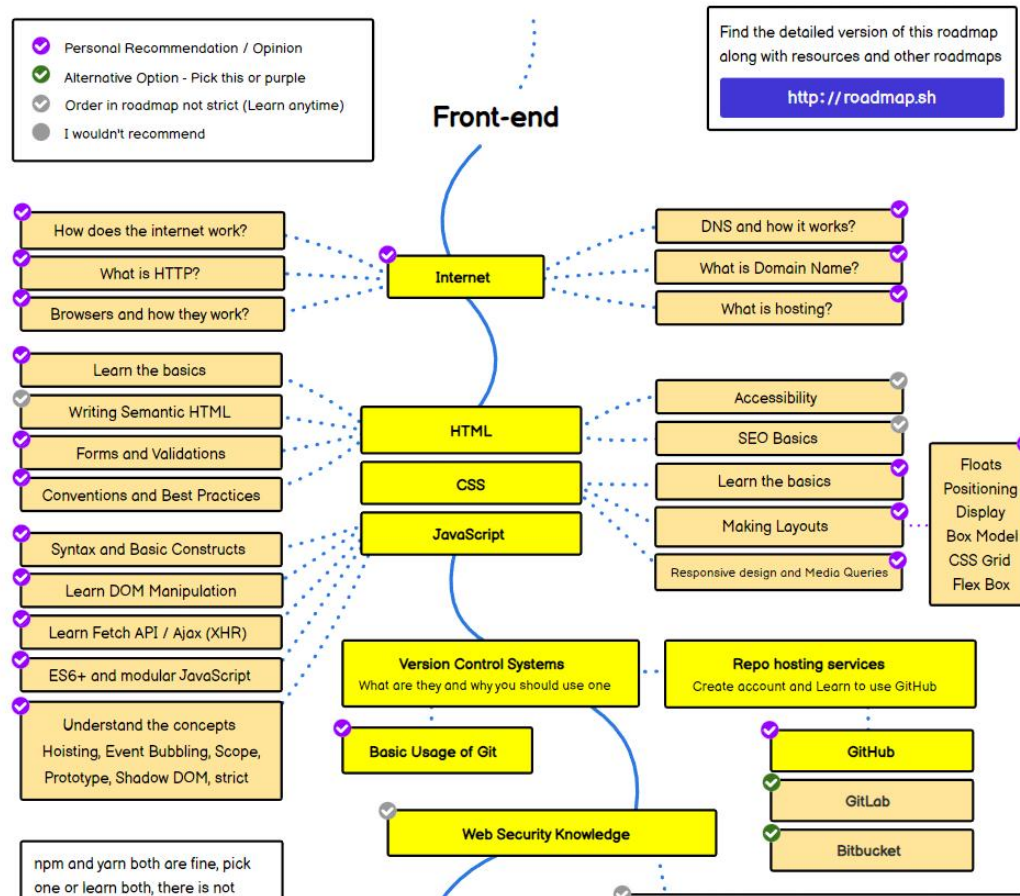
План курса

18 лекций, 8 лабораторных работ

- HTML (3)
- CSS (2)
- JS (2)
- ReactJS (2)
- Архитектуры веб-приложений
- Аутентификация
- Уязвимости (3)
- Методика тестирования

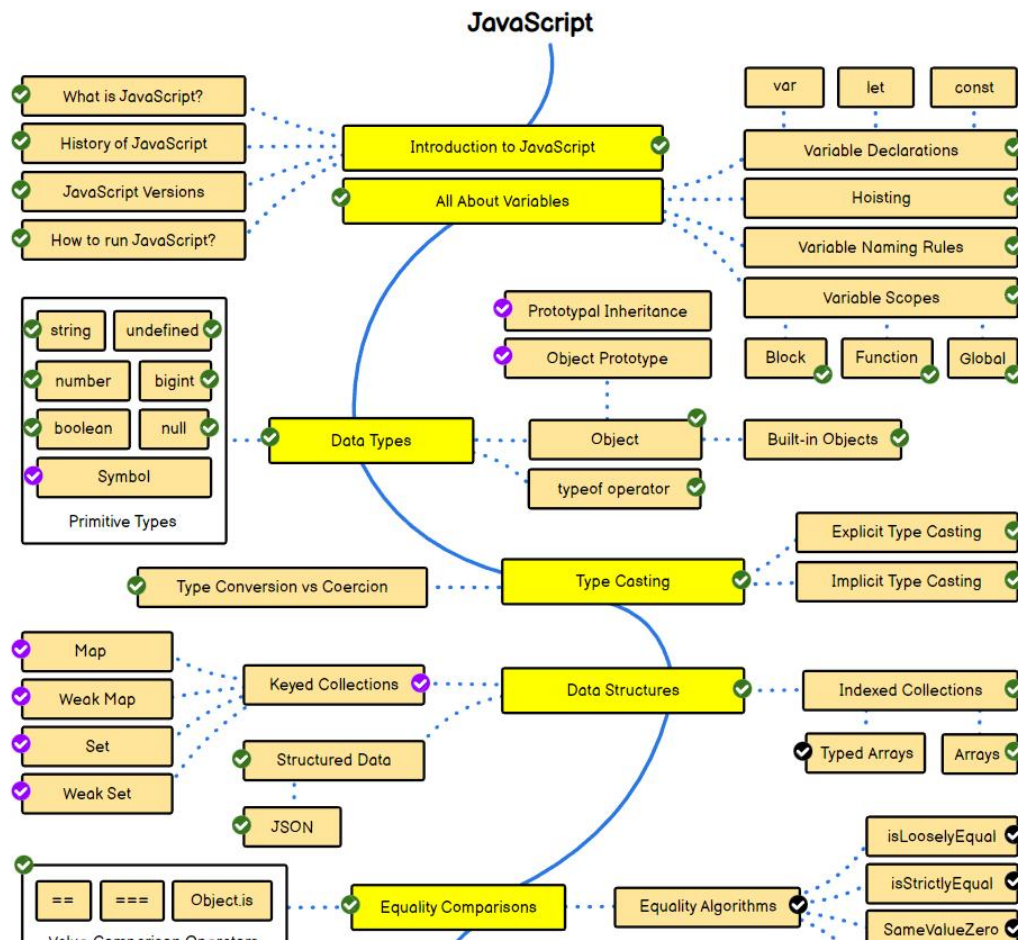
Траектории развития

<https://roadmap.sh/frontend>



Траектории развития

<https://roadmap.sh/javascript>



Где учиться помимо лекций

Интерактивные курсы HTML, CSS, JS:

— <https://www.w3schools.com/>

Справочники на русском:

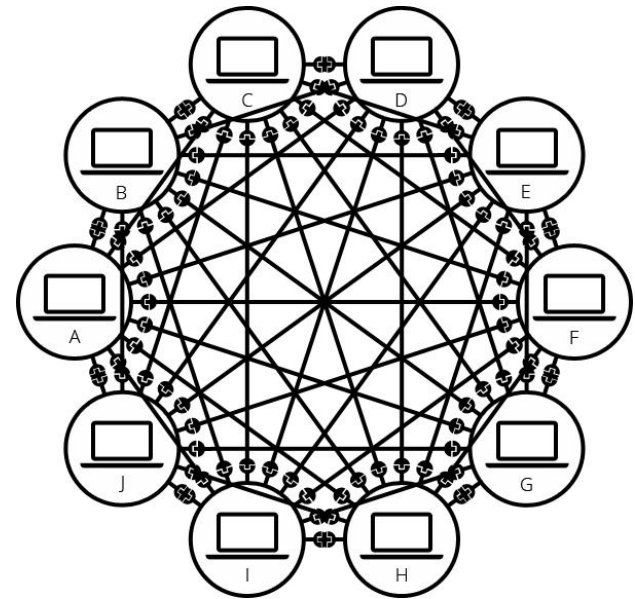
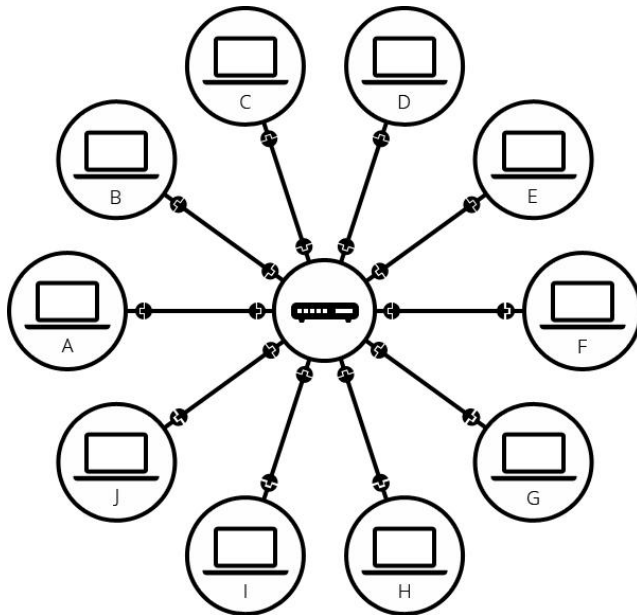
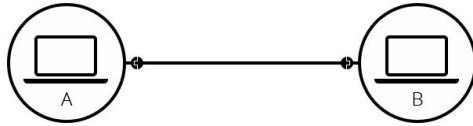
— <http://htmlbook.ru/>

— <https://learn.javascript.ru/>

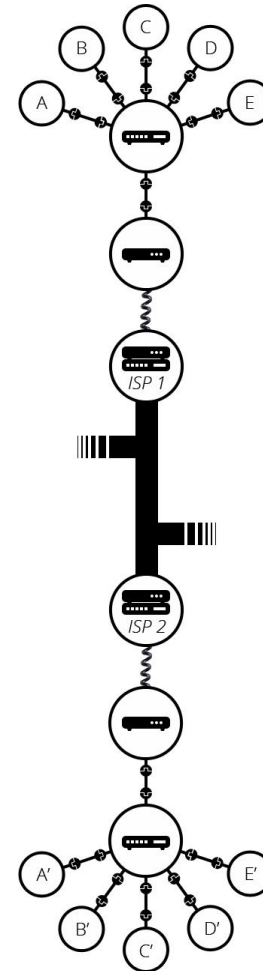
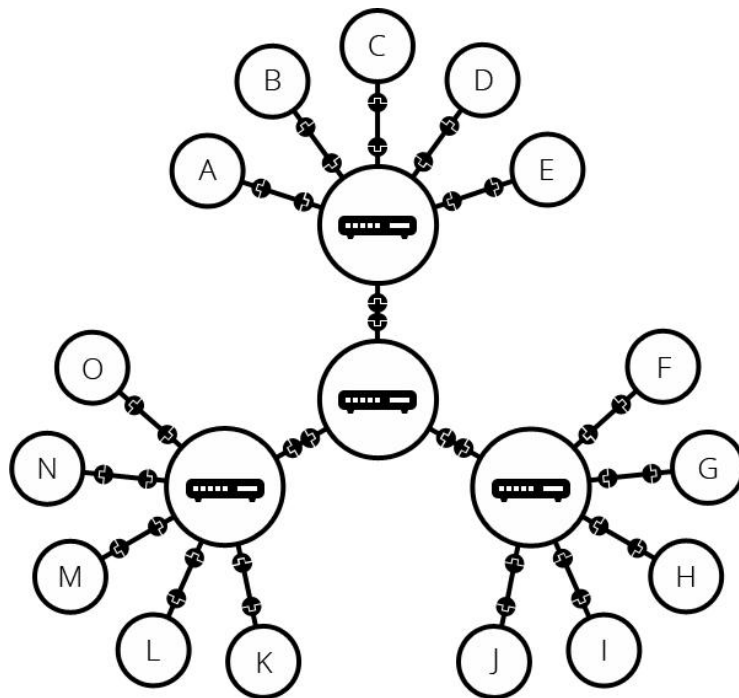
По уязвимостям:

— <https://owasp.org/www-project-top-ten/>

Как устроен интернет



Как устроен интернет



Протоколы передачи данных

уровень	протоколы
канальный	Ethernet, IEEE 802
сетевой	IPv4, IPv6
транспортный	TCP
прикладной	HTTP, SMTP, POP3, FTP, TELNET

IP-адрес: 142.251.1.113

Web = TCP/IP + HTTP + HTML

DNS

Система Доменных Имен

google.com →

обращение к DNS-серверу →

получение адреса →

HTTP запрос к 142.251.1.113

Протокол HTTP

Язык общения браузеров и серверов в Web

GET / HTTP/1.1

Host: www.opera.com

HTTP/1.1 200 OK

Date: Wed, 23 Nov 2011 19:41:37 GMT

Server: Apache

Content-Type: [text/html](#); charset=utf-8

Set-Cookie: language=none; path=/; domain=www.opera.com; expires=Thu, 25-Aug-2011 19:41:38 GMT

Set-Cookie: language=en; path=/; domain=.opera.com; expires=Sat, 20-Nov-2021 19:41:38 GMT

Vary: Accept-Encoding

Transfer-Encoding: chunked

<!DOCTYPE html>

<html lang="en">

...

Анатомия HTTP запроса

- URL - Uniform Resource Locator
- Тип запроса: GET, POST, OPTIONS, HEAD, PUT, DELETE, TRACE, CONNECT
- Заголовки запроса
- Тело запроса
- Статус ответа: 200, 302, 404, 403, 503
- Заголовки ответа
- Тело ответа

URL

http://www.example.com:80/path/to/myfile.html?key1=value1
&key2=value2#SomewhereInTheDocument

http://www.example.com:80/path/to/myfile.html?key1=value1
&key2=value2#SomewhereInTheDocument

→ Scheme

http://www.example.com:80/path/to/myfile.html?key1=value1
&key2=value2#SomewhereInTheDocument

→ Domain Name

→ Port

http://www.example.com:80/path/to/myfile.html?key1=value1
&key2=value2#SomewhereInTheDocument

→ Path to resource

http://www.example.com:80/path/to/myfile.html?key1=value1
&key2=value2#SomewhereInTheDocument

→ Parameters

http://www.example.com:80/path/to/myfile.html?key1=value1
&key2=value2#SomewhereInTheDocument

→ Anchor

Cookies

Информация, хранимая в браузере, связанная с доменом.

Зачем нужны:

- повышение удобства работы пользователей (авторизация)
- сбор статистики

Типы куков:

- сессионные
- постоянные
- защищенные

```
Cookie: _ym_uid=158089380; AddressRegistry_DetailView_Main_Tabs=0; QuarryBorder_DetailView_Main_Tabs=0; GarbageIllegalPossibility_DetailView_Main_Item1_Tabs=0; Process_DetailView_Main_Tabs=0; TimberSection_DetailView_Main_Item1_Tabs=0; QuarryLand_DetailView_Main_Item2_Tabs=0; QuarryLicensedSite_DetailView_Main_Tabs=0; Gis2Addresses_DetailView_Main_Tabs=0; __utmz=224886924.1644911626.457.6.utmcsr=google|utmccn=(organic)|utmcmd=organic|utmctr=(not%20provided); __utma=224886924.2135476556.1603170278.1646393279.1646811576.474; QuarryUnalottedOffence_DetailView_Main_Tabs=0; ASP.NET_rk_SessionId=fjblt05r; :zllq; 2aa6c8c7-7b16-4114-b613-642572562c77=unloaded; ASP.NET_SessionId=4poeij; o; e8d5523e-cc18-4e13-91b4-a30f4544745e=unloaded; 4d541d3d-19a8-4fa0-bce6-d8f6f1e1fa76=unloaded; _ga=GA1.1.357435934.1616757046; 94227891-18f2-4dfa-b730-52b52d3150d4=unloaded; Revision_DetailView_Main_Tabs=0; d0e15b4c-6ed1-4a9f-847a-400c1d114867=unloaded; 56ae0552-a5ad-4767-96c2-ba63391b29bb=unloaded; b80b4611-ced8-4eb0-b847-a06aa18a13d0=unloaded; 91b8cfa1-8c68-4a63-8942-cbdd4f2957b4=unloaded; b844f718-1a41-4a4d-827a-7ba08efcd4e3=unloaded; eee71a8e-6b12-4f9e-a44c-b70f2aa40ee5=unloaded; 5a80eee1-5640-4887-aef9-630dec955ce7=unloaded; AgroUnused_DetailView_Main_Tabs=0; c9ea8cea-4dbf-4d38-9b00-fb22c3171d9e=unloaded; ce7800b7-92f5-4553-89ed-b369348fbd30=unloaded; d7572bdb-93a3-4021-bdf7-9d31cc547a7b=unloaded; 7e1426cb-f784-4cf0-baa4-2bb6122ac435=unloaded; 586712ce-bd08-437c-81a1-b1b97e883e1a=unloaded; a39e58b3-87e2-4ff1-9062-f202a5dfb48c=unloaded; 62c78394-0235-421c-9c37-24781993408b=unloaded; e2a9ade9-2db8-4280-9686-a372149f0874=unloaded; 491fbcd8-ceb9-4993-a1d4-f6505a332853=unloaded; af002b62-b5fd-4686-af5d-14533cc9e278=unloaded; TimberSubsection_DetailView_Main_Item2_Tabs=0; 1d4b09cd-e290-4f75-8fb4-280cc4bfb9a1=unloaded; 29918a46-11ec-475e-abel-26c2505d2533=unloaded; rkLogin=04029598A; B036CB27C2E9894FCB3D532AEF30C3D5D5ACD867E9EE9EDE2FA243A6E79EF5B47A9904397F95D42371BDA792237A7F39BA6A9B0E4553F2F0145D10DE0A078140037684AEB2C1A03360E3B4FB3AEA8EC578E2327538FD929E9FA7E04164E69306395431F84C47496568916709F9822ED7A5D9A08185CE0F1D5D77F57368; NrIzhMonitoring_DetailView_Main_SizeableEditors_Tabs=6; 7ddfd79a-5fbc-4684-87b7-87dd9f3b5377=unloaded; _ym_d=1661323596; 6006a231-0fd5-4457-bd21-7ef2a88cf98d=unloaded; e8717f67-9939-495f-97a9-54ef27af14a1=unloaded; 139856c5-043f-4d24-978b-ac5d8612648c=unloaded; Login=13776; 1E B55C20D2212CA3B045AC7986EDB3E876039686814CE68A2D9F9C0272B49D178E17A2F885C83522774700043AC4B85D06814E89A71DF70A2147F53346DA359A4B48AAE1AB3E4A85187D04DA93A91D39B21729B6CAFE6DCC28F18DBE75E6C0A2D5C871848924FDE81887612ACFD124D0048CCDE64F91B18C4D29330AE8B607136AC38BE3436C1EDD27E8E9678E25; ddc5a23-f8b7-4d9f-ac97-647891f67d29=unloaded; b6129122-df66-444c-9978-cfd979791127=unloaded; JSESSIONID=C77FDD9034; CF; _ga_PW8MXRZ8EM=GS1.1.1662102863.70.1.1662102865.0.0.0
```

Браузеры

Приложение для отображения Web-страниц.

Среда исполнения для браузерных приложений.






















Chrome, Firefox, Opera, Edge, Safari, мобильные версии тех же самых

Различаем термины:

Web-страница, Web-сайт, Web-сервер

Как браузер загружает страницу

- пользователь ввел адрес
- браузер узнал IP у DNS
- сделал HTTP запрос
- в зависимости от ответа порождает новые запросы
- отображает полученное HTML+CSS+медиа
- исполняет программный код

Name	Status	Domain	Type
 samis.geosamara.ru	200	samis.geosamara.ru	document
 fonts.css	200	samis.geosamara.ru	stylesheet
 main.css	200	samis.geosamara.ru	stylesheet
 corrections.css	200	samis.geosamara.ru	stylesheet
 details-shim.min.css	200	samis.geosamara.ru	stylesheet
 jquery-1.11.2.min.js	200	samis.geosamara.ru	script
 app.js	200	samis.geosamara.ru	script
 details-shim.min.js	200	samis.geosamara.ru	script
 jquery.sliderTabs.css	200	samis.geosamara.ru	stylesheet
 jquery.sliderTabs.js	200	samis.geosamara.ru	script
 logo.png	200	samis.geosamara.ru	png
 37ba34aed9165214b1e639e73764d5e3.png	200	samis.geosamara.ru	png
 gis-svgk.png	200	samis.geosamara.ru	png
 %D0%94%D0%BE%D1%81%D1%82%D1%83%D0%B...	200	samis.geosamara.ru	png
 plugin-blue.png	200	samis.geosamara.ru	png
 plugin-blue.png	200	samis.geosamara.ru	png
 gis-samara.png	200	samis.geosamara.ru	png
 mouse_blue_72x72.png	200	samis.geosamara.ru	png
 support.png	200	samis.geosamara.ru	png
 poster-01.jpg	200	samis.geosamara.ru	jpeg
 poster-02.jpg	200	samis.geosamara.ru	jpeg

Веб-серверы

Приложение для обработки HTTP-запросов:
Apache, IIS, Tomcat, nginx, ...

Роли:

- раздача статики
- динамические запросы (сервер приложений)
- потоковые раздачи

HTML

Hypertext Markup Language – язык разметки для структурирования и отображения веб-страницы и её контента

```
<ul class="b-menu b-menu_sites">
  <li class="b-menu__item is-current">
    <a href="http://samis.geosamara.ru/" title="Самара-Информспутник">Самара-Информспутник</a>
    <div class="b-menu__detailed">
      <div class="b-menu__go">
        <a href="http://samis.geosamara.ru/">перейти на сайт</a>
      </div>
    </div>
  </li>
  <li class="b-menu__item">
```

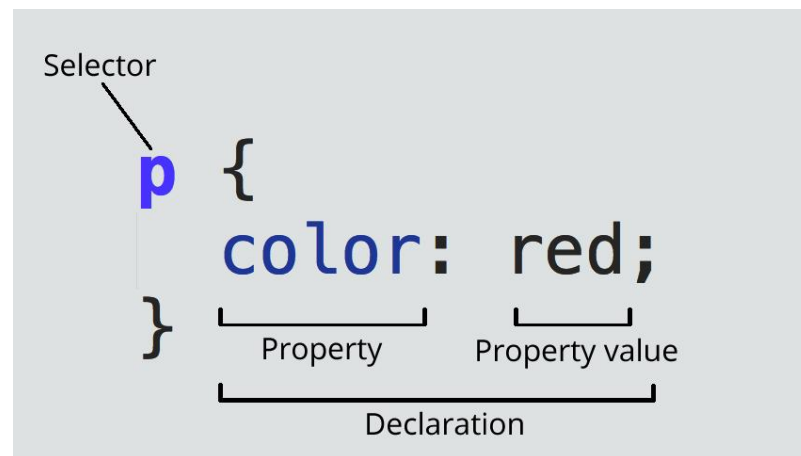
Теги: <html>, <div>, <p>, <a>, , <script>, ...

Аттрибуты: id, class, href, style, ...

CSS

Cascading Style Sheets – язык описания стилей для элементов HTML

```
.l-wrapper {  
  padding: 0 80px;  
  background: #f0f2f4;  
}  
  
.l-wrapper_ipsi {  
  background: #fff url("../img/patterns/layout-background-lgradient-i.png") repeat-x top left;  
  border-top: 1px solid #dbd8cc;  
}  
  
.l-grid .l-grid__col {  
  display: block;  
  float: left;  
  vertical-align: top;  
}
```



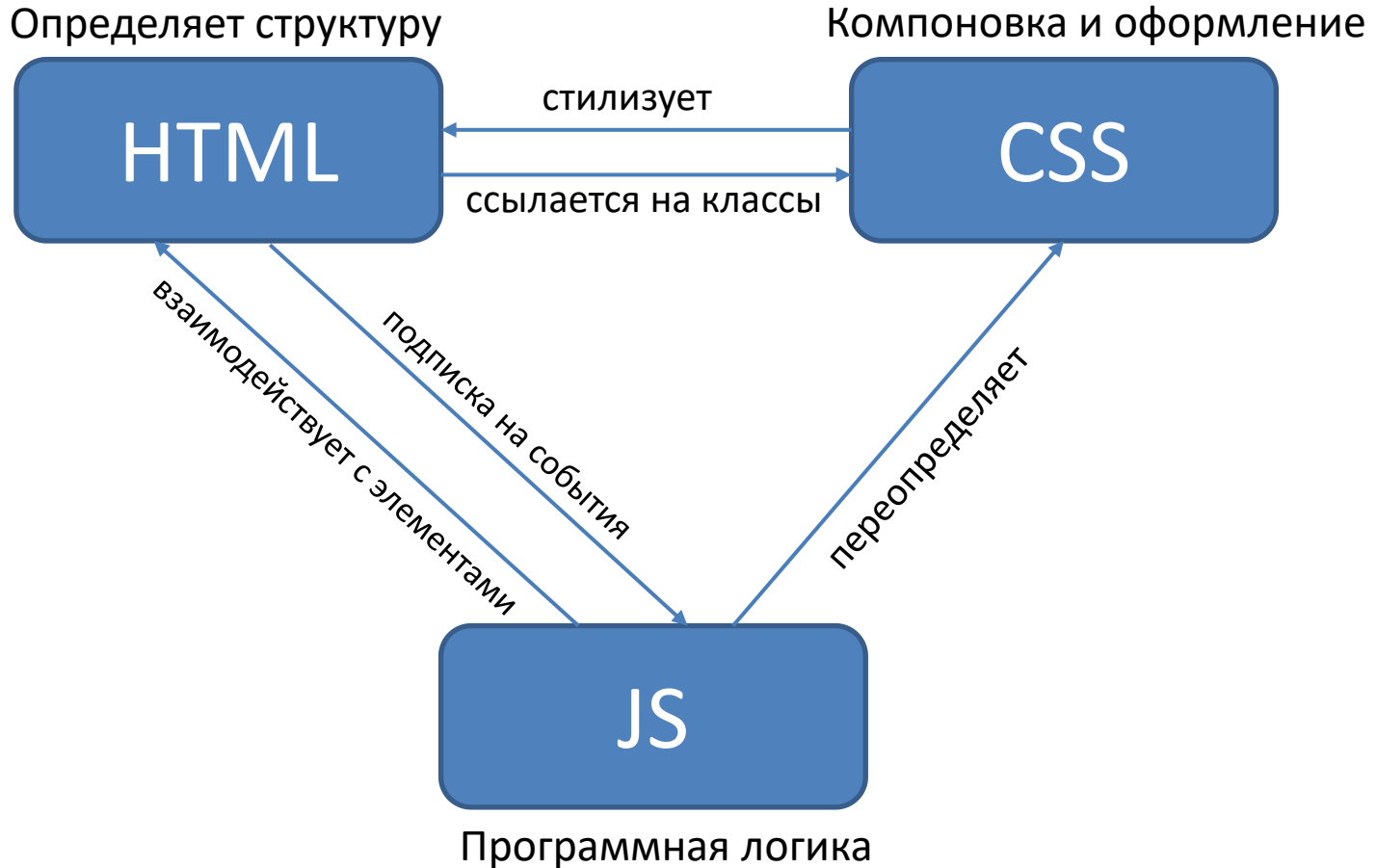
JavaScript

Скриптовый язык, исполняемый на web-странице.

- интерактивные действия
- динамическая подгрузка контента
- сложная стилизация
- «rich internet applications»

```
$(function() {  
    $('body')  
        .on('click', '.js-show-all-tags', function() {  
            var $this = $(this);  
            var $parent = $this.closest('.b-rubricator');  
  
            if ($parent.hasClass('is-expanded')) {  
                $parent.removeClass('is-expanded');  
                $this.text('все теги ↓')  
            }  
            else {  
                $parent.addClass('is-expanded');  
                $this.text('свернуть ↑')  
            }  
        })  
    })  
})
```

Что происходит в браузере



Инструменты для разработки

- Текстовый редактор (VS Code или по вкусу)
- Браузер (отладка – F12)
- Локальный веб-сервер (статика – nginx, динамика – Apache, Tomcat, IIS)
- Git
- справочники по ссылкам со слайда 5 (или из itsecd/websec)