

# AJAX



Web.Dev.  
Courses

[vk.com/web\\_dev\\_courses](https://vk.com/web_dev_courses)  
[web.dev.courses.dp.ua/ort/](https://web.dev.courses.dp.ua/ort/)

# Интеграция

*Как вставить на сайт  
модуль  
комментариев от Facebook.*

[https://developers.facebook.com/docs/plugins/comments?locale=ru\\_RU](https://developers.facebook.com/docs/plugins/comments?locale=ru_RU)

https://developers.facebook.com/docs/plugins/comments?locale=ru\_RU

Developers My Apps Products Docs Tools & Support News Search in docs Log In

Product Docs  
Ads for Apps  
Ads for Websites  
Ссылки на приложение  
Audience Network  
Игры  
Insights  
Вход  
Marketing API  
Платежи  
Sharing  
Веб  
iOS  
Android  
Custom Stories  
Социальные плагины  
Кнопка «Нравится» (Сеть)  
Like Button (iOS)  
Like Button (Android)  
Share Button  
Send Button  
Embedded Posts  
Кнопка «Подписаться»

Settings  
FAQ

## Comments

The Comments box lets people comment on content on your site using their Facebook profile and shows this activity to their friends in news feed. It also contains built-in moderation tools and special social relevance ranking.

URL to comment on  Width

Number of Posts  Color Scheme

7 360 комментариев

Добавить комментарий...

Комментарий

**Nikita Wüst** · Geschäftsführer в Umzüge und Kleintransporte N.Wüst und E. Suchomlinov GbR  
0222  
Ответить · Нравится · 7 ноября 2014 г. в 13:15

**Antwan Gauge Calibre Turman** · Lyu · 6 823 подписчика  
4sho  
Ответить · Нравится · 10 января в 12:41

**Max Maximov** · УрГУПС  
спasibo za webinar  
Ответить · Нравится · 7 ноября 2014 г. в 14:28

Просмотреть еще 7 319

Get Code

Генератор кода для вставки на сайт

ce Network

Your Plugin Code ✕

[HTML5](#) [XFBML](#) [IFRAME](#) [Адрес](#)

Include the [JavaScript SDK](#) on your page once, ideally right after the opening `<body>` tag.

```
<div id="fb-root"></div>
<script>(function(d, s, id) {
  var js, fjs = d.getElementsByTagName(s)[0];
  if (d.getElementById(id)) return;
  js = d.createElement(s); js.id = id;
  js.src = "//connect.facebook.net/ru_RU/sdk.js#xfbml=1&version=v2.0";
  fjs.parentNode.insertBefore(js, fjs);
})(document, 'script', 'facebook-jssdk');</script>
```

Place the code for your plugin wherever you want the plugin to appear on your page.

```
<div class="fb-comments" data-
href="http://developers.facebook.com/docs/plugins/comments/" data-
numposts="5" data-colorscheme="light"></div>
```

ing API

ки

g

oid

om Sto

мальнв

опка «f

еть)

e Butto

e Butto

are But

nd Button

bedded Posts

*Генератор кода для вставки на*

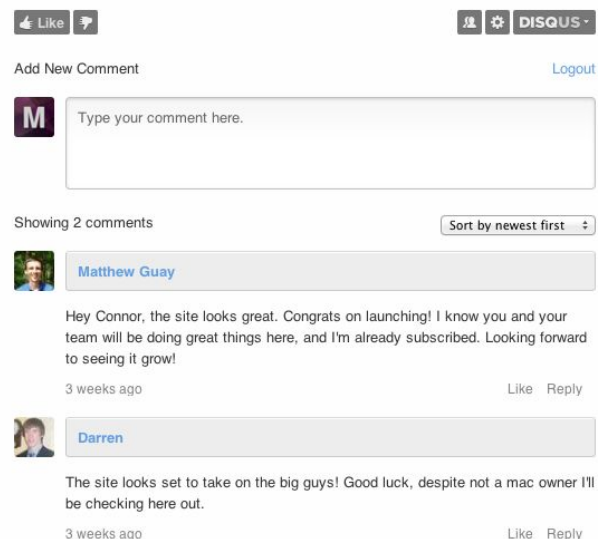
Сгенерированный код необходимо вставить в страницу сайта.

```
1 <?php get_header(); the_post(); ?>
2 <div id="fb-root"></div>
3 <script>(function(d, s, id) {
4     var js, fjs = d.getElementsByTagName(s)[0];
5     if (d.getElementById(id)) return;
6     js = d.createElement(s); js.id = id;
7     js.src = "//connect.facebook.net/ru_RU/sdk.js#xfbml=1&version=v2.0";
8     fjs.parentNode.insertBefore(js, fjs);
9 }) (document, 'script', 'facebook-jssdk');</script>
10 <h2><a href="<?php bloginfo('url'); ?>">
11     Новости</a> / <?php the_title(); ?></h2>
12 <div>
13     <span>#<?php the_ID(); ?></span>
14     <span class="news-info"><?php the_time('d.m.Y G:i'); ?></span>
15     <div><?php the_content(); ?></div>
16 </div>
17 <div class="fb-comments" data-href="<?php the_permalink(); ?>"
18     data-numposts="5" data-colorscheme="light"></div>
19 <?php get_footer(); ?>
```

Модернизированная версия:  
*single.php*

# Домашнее задание

Познакомится с *Disqus* – один из лучших механизмов комментариев для сайтов.



<https://disqus.com>

Вариант #1

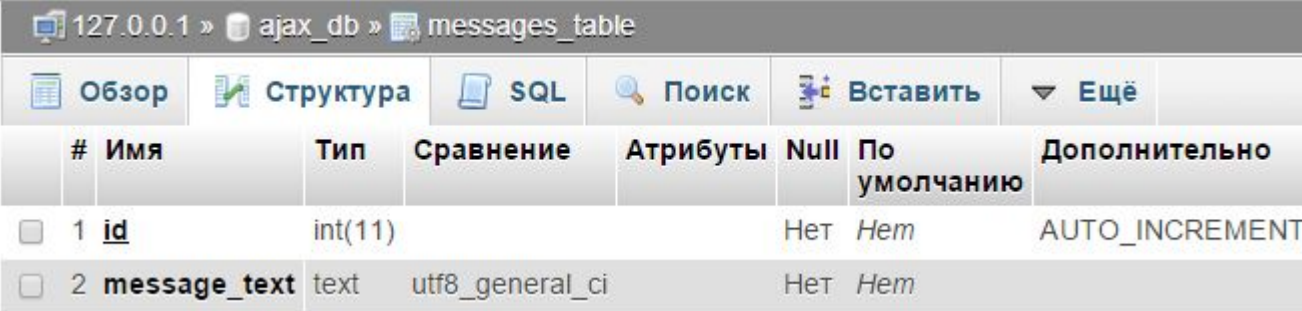


# Подготовьте базу данных и проект в

Денвере.  
Название:

Таблица: «messages\_table»

Структура:



#	Имя	Тип	Сравнение	Атрибуты	Null	По умолчанию	Дополнительно
<input type="checkbox"/>	1 <u>id</u>	int(11)			Нет	Нет	AUTO_INCREMENT
<input type="checkbox"/>	2 <u>message_text</u>	text	utf8_general_ci		Нет	Нет	

SQL:

```
CREATE TABLE IF NOT EXISTS `messages_table` (  
  `id` int(11) NOT NULL AUTO_INCREMENT,  
  `message_text` text NOT NULL, PRIMARY KEY (`id`))  
ENGINE=InnoDB DEFAULT CHARSET=utf8 AUTO_INCREMENT=77 ;
```

Каталог в Денвер:

[ajax.dp.ua/www](http://ajax.dp.ua/www)

# Простейший

## чат

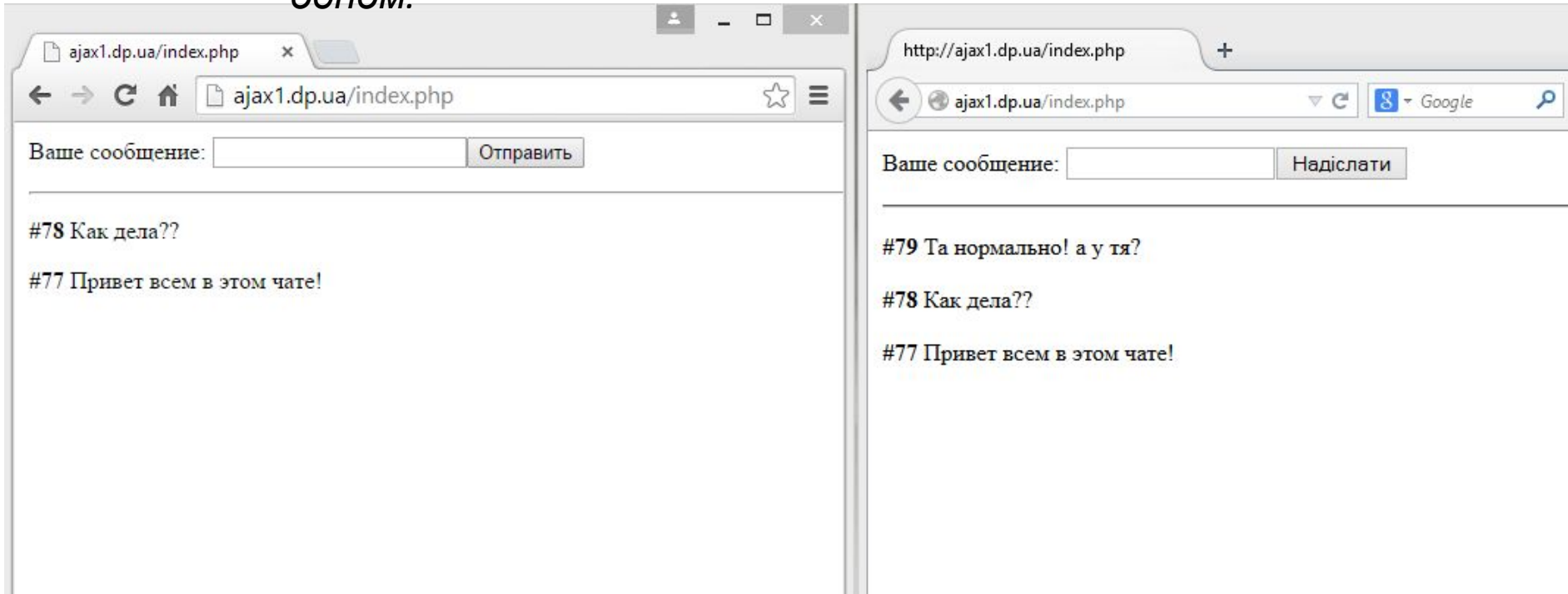
```
1 <?php //Сохраните файл как UTF-8 (без BOM).
2     mysql_connect('localhost', 'root', '');
3     mysql_select_db('ajax_db');
4
5     if(strlen($_REQUEST['sms']) > 1){
6         $sms = mysql_real_escape_string($_REQUEST["sms"]);
7         mysql_query("INSERT INTO `messages_table` (`message_text`) VALUES ('$sms')");
8         header('Location: ./index.php');
9     }
10
11     $result = mysql_query("SELECT * FROM `messages_table` ORDER BY `id` DESC LIMIT 20");
12     header('Content-Type: text/html; charset=utf-8');
13 >?
14 <html><head>
15
16 <style> body{ width:800px; margin:0 auto; padding: 10px; } </style></head>
17 <body>
18 <form>
19     Ваше сообщение: <input type="text" name="sms"><input type="submit">
20 </form>
21 <hr />
22 <div id="messages">
23     <?php while($one_message = mysql_fetch_array($result)){ ?>
24     <p>
25         <b>#<?php echo $one_message['id']; ?></b>
26         <?php echo $one_message['message_text']; ?>
27     </p>
28     <?php } ?>
29 </div>
30 </body></html>
```

*index.php*

# Простейший

## чат

Откройте в двух браузерах, напишите сообщение в одном.



**В чём проблема:** при отправке сообщения, другие участники чата получают сообщение только когда обновят страницу (самостоятельно или после отправки сообщения).

# Простейший

16.1a

Чат+

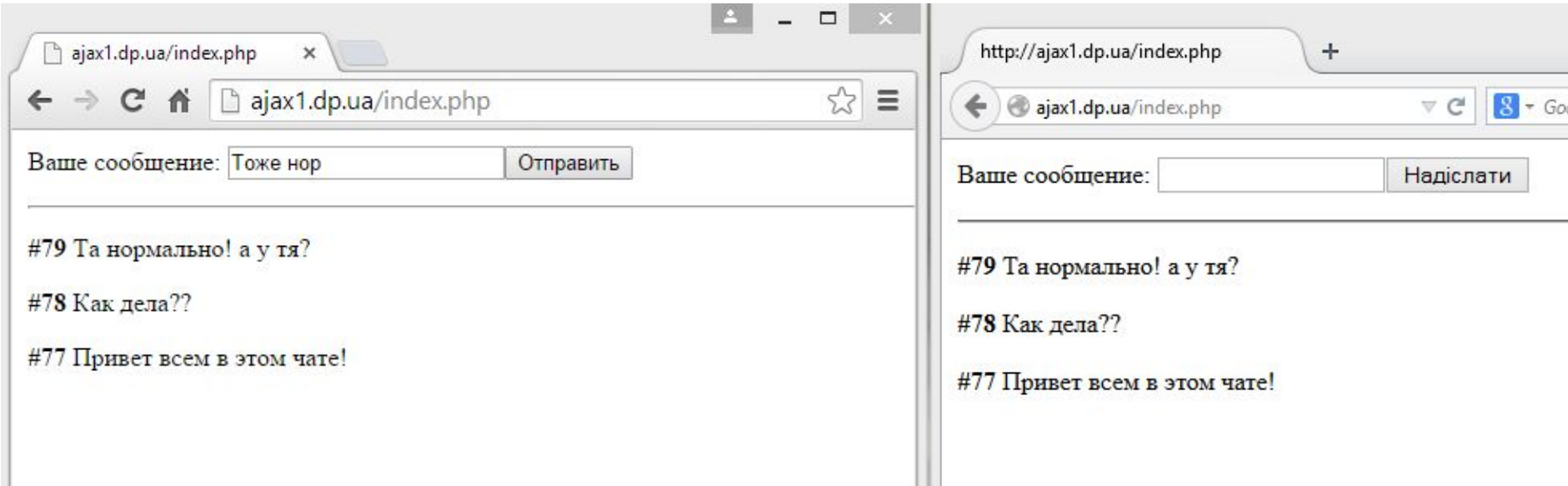
```
1 <?php //Сохраните файл как UTF-8 (без BOM).
2     mysql_connect('localhost', 'root', '');
3     mysql_select_db('ajax_db');
4
5     if(strlen($_REQUEST['sms']) > 1){
6         $sms = mysql_real_escape_string($_REQUEST["sms"]);
7         mysql_query("INSERT INTO `messages_table` (`message_text`) VALUES ('$sms')");
8         header('Location: ./index.php');
9     }
10
11     $result = mysql_query("SELECT * FROM `messages_table` ORDER BY `id` DESC LIMIT 20");
12     header('Content-Type: text/html; charset=utf-8');
13 >?>
14 <html><head>
15     <meta http-equiv="refresh" content="5">
16     <style> body{ width:800px; margin:0 auto; padding: 10px; } </style></head>
17 <body>
18     <form>
19         Ваше сообщение: <input type="text" name="sms"><input type="submit">
20     </form>
21     <hr />
22     <div id="messages">
23         <?php while($one_message = mysql_fetch_array($result)){ ?>
24             <p>
25                 <b>#<?php echo $one_message['id']; ?></b>
26                 <?php echo $one_message['message_text']; ?>
27             </p>
28             <?php } ?>
29     </div>
30 </body></html>
```

*index.php*

12

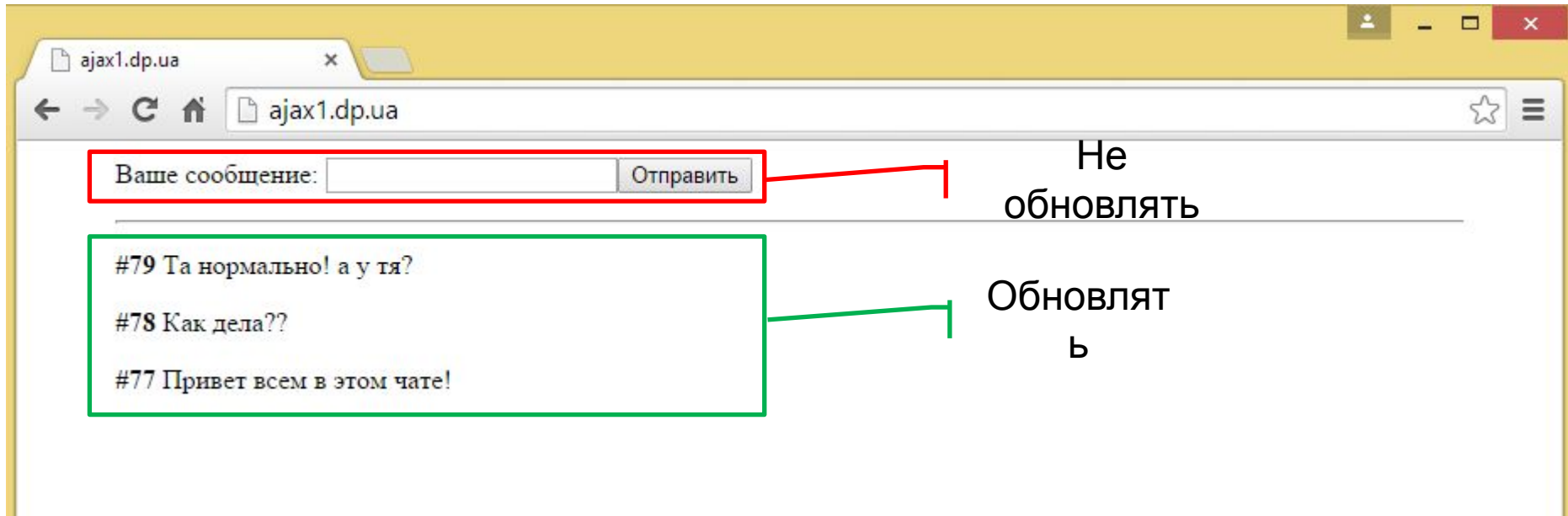
# Простейший

**чат**  
Откройте в двух браузерах, напишите сообщение в одном.



**В чём теперь проблема:** при отправке сообщения, другие участники чата получают его автоматически, но теперь проблематично набрать сообщение.

# Простейший чат+



*Хорошо бы обновлять только часть страницы не затрагивая другую.*

Вариант #2

# Простейший чат 2.0

16.2

```
1 <?php
2     header('Content-Type: text/html; charset=utf-8');
3
4     mysql_connect('localhost', 'root', '');
5     mysql_select_db('ajax_db');
6
7     $result = mysql_query("SELECT * FROM `messages_table` ORDER BY `id` DESC LIMIT 20");
8
9     while($one_message = mysql_fetch_array($result)){
10    ?>
11    <p>
12
13        <b>#<?php echo $one_message['id']; ?></b>
14
15        <?php echo $one_message['message_text']; ?>
16
17    </p>
18 <?php } ?>
```

*get\_data.php*

16



# Простейший чат

16.3

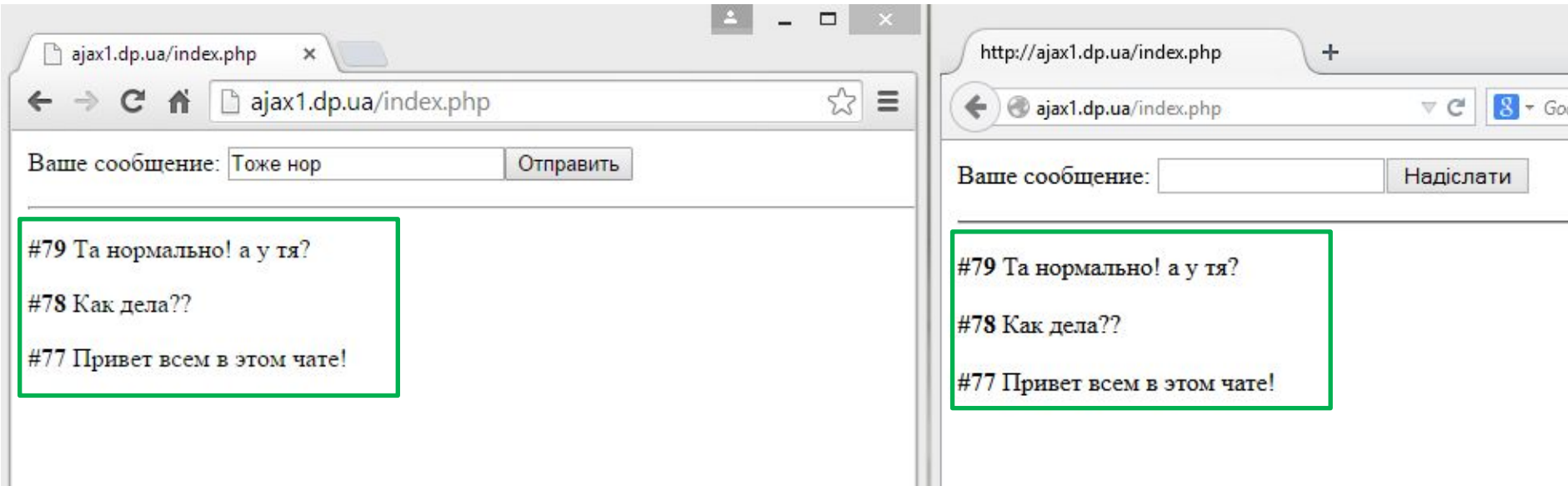
```
1 <?php //Сохраните файл как UTF-8 (без BOM).
2     mysql_connect('localhost', 'root', '');
3     mysql_select_db('ajax_db');
4
5     if(strlen($_REQUEST['sms']) > 1){
6         $sms = mysql_real_escape_string($_REQUEST["sms"]);
7         mysql_query("INSERT INTO `messages_table` (`message_text`) VALUES ('$sms')");
8         header('Location: ./index.php');
9     }
10    header('Content-Type: text/html; charset=utf-8');
11    ?>
12 <html><head>
13 <script>
14     window.onload = function(){
15         async_load_data();
16         setInterval(async_load_data, 3000);
17     };
18
19     function async_load_data(){
20         var XHR = new XMLHttpRequest();
21         XHR.onload = function(){
22             document.getElementById("messages").innerHTML = XHR.responseText;
23         };
24         XHR.open("get", "get_data.php", true);
25         XHR.send();
26     };
27 </script>
28 <style> body{ width:800px; margin:0 auto; padding: 10px; } </style></head>
29 <body>
30     <form>
31         Ваше сообщение: <input type="text" name="sms"><input type="submit">
32     </form>
33     <hr />
34     <div id="messages">
35     </div>
36 </body></html>
```

*index.php*

17

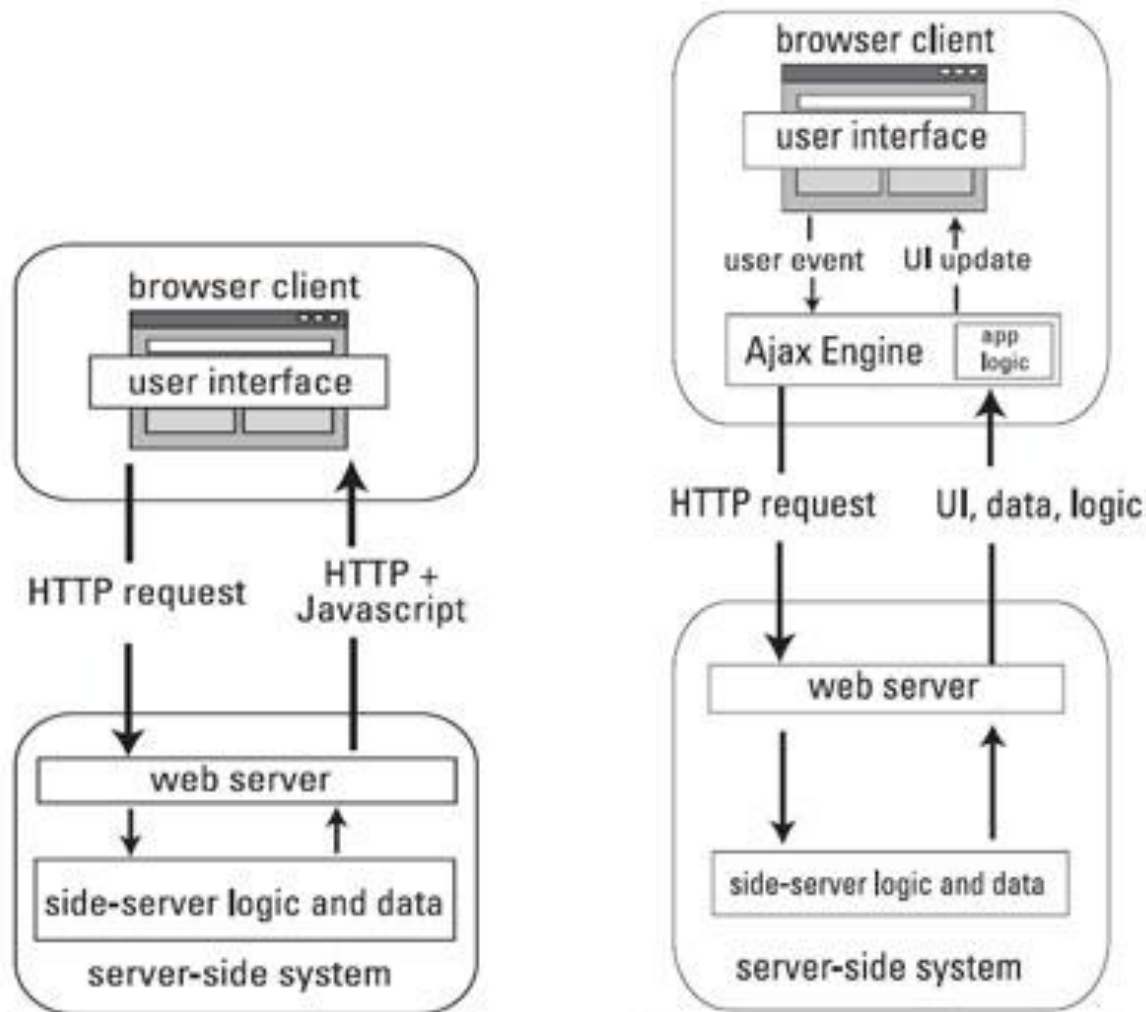
# Простейший чат

Откройте в ~~двух~~<sup>3х</sup> браузерах, напишите сообщение в одном.



Теперь часть страницы обновляется каждый 3 секунды, тем самым обеспечивая подгрузку свежих сообщений, при этом ничего не мешает набирать сообщение.

**AJAX, Ajax** (от англ. **A**synchronous **J**avascript and **X**ML — «асинхронный JavaScript и XML») — подход к построению интерактивных пользовательских интерфейсов веб-приложений, заключающийся в «фоновом» обмене данными браузера с веб-сервером. В результате, при обновлении данных веб-страница не перезагружается полностью, и веб-приложения становятся быстрее и удобнее.



The image shows a web browser window with the URL `ajax2.dp.ua`. The page content includes a form with the label "Ваше сообщение:" and a button "Отправить". Below the form, there are three chat messages:

- #79**Та нормально! а у тя?
- #78**Как дела??
- #77**Привет всем в этом чате!

The browser's developer tools are open, showing the DOM tree. The `<body>` element is selected, and its structure is as follows:

```
<html>
  <head>...</head>
  <body>
    <form>...</form>
    <hr>
    <div id="messages">
      <p>
        <b>#79</b>
        "Та нормально! а у тя?"
      </p>
      <p>
        <b>#78</b>
        "Как дела??"
      </p>
      <p>
        <b>#77</b>
        "Привет всем в этом чате!"
      </p>
    </div>
  </body>
</html>
```

The image shows a web browser window with the address bar displaying 'ajax2.dp.ua'. The page content consists of a text input field labeled 'Ваше сообщение:' with an 'Отправить' button, and a chat log with three messages: '#79 Та нормально! а у тя?', '#78 Как дела??', and '#77 Привет всем в этом чате!'. Below the page content, the browser's developer tools are open to the 'Network' tab. The network log shows a list of requests to 'ajax2.dp.ua' and 'get\_data.php'. The selected request is a GET request to 'http://ajax2.dp.ua/get\_data.php' with a status code of 200 OK. The 'Request Headers' section is expanded, showing: Accept: \*/\*, Accept-Encoding: gzip, deflate, sdch, Accept-Language: ru-RU,ru;q=0.8,en-US;q=0.6,en;q=0.4,uk;q=0.2, Connection: keep-alive, Host: ajax2.dp.ua, Referer: http://ajax2.dp.ua/, User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/39.0.2171.99 Safari/537.36. The 'Response Headers' section is also expanded, showing: Connection: Keep-Alive, Content-Length: 186, Content-Type: text/html; charset=utf-8, Date: Tue, 20 Jan 2015 18:35:15 GMT, Keep-Alive: timeout=5, max=58, Server: Apache/2.2.22 (Win32) mod\_ssl/2.2.22 OpenSSL/1.0.1c PHP/5.3.13, X-Powered-By: PHP/5.3.13. At the bottom left of the developer tools, it indicates '6 requests | 3.1 KB transferr...'. The browser's address bar and navigation buttons are visible at the top.

Вариант #3

# Реальный чат в чистом виде, без jQuery

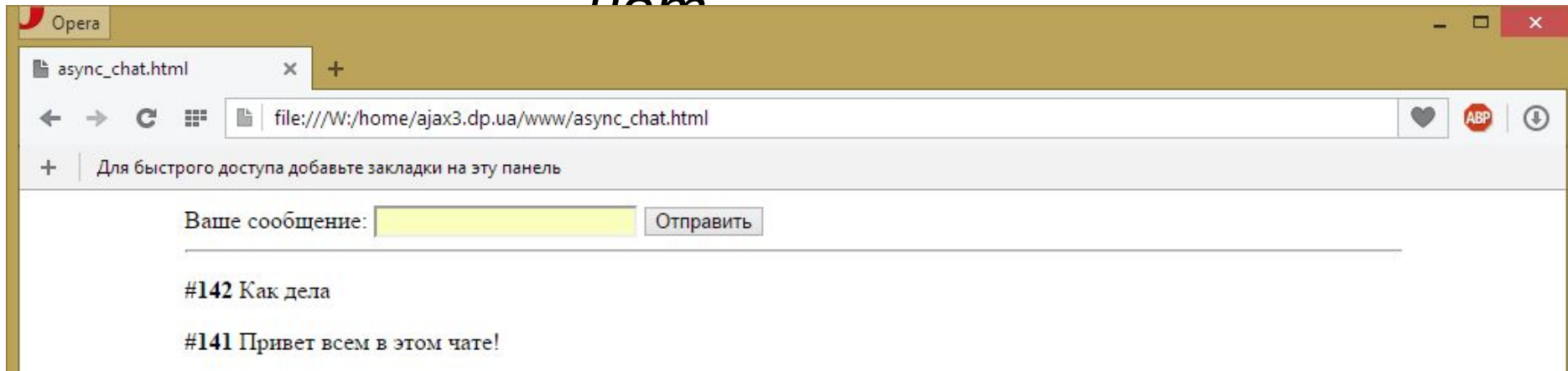
## Создайте обычный HTML файл в UTF-8 с

```
1 <html><head>
2 <script>
3   window.onload = function(){
4     async_load_data(); //Первичная загрузка данных
5     setInterval(async_load_data, 3000);
6     document.getElementById("send_btn").onclick = async_send_data;
7   };
8
9   function async_send_data(){
10    btn = document.getElementById('send_btn');
11    sms = document.getElementById("sms");
12
13    btn.disabled = true;
14
15    var virtual_from = new FormData();
16    virtual_from.append("sms", sms.value);
17
18    var XHR = new XMLHttpRequest();
19    XHR.onload = function(){
20      sms.value = "";
21      btn.disabled = false;
22      async_load_data();
23    };
24    XHR.open("post", "http://web.dev.courses.dp.ua/ort/ajax/add_data.php", true);
25    XHR.send(virtual_from);
26  };
27
28  function async_load_data(){
29    var XHR = new XMLHttpRequest();
30    XHR.onload = function(){
31      document.getElementById("messages").innerHTML = XHR.responseText;
32    };
33    XHR.open("get", "http://web.dev.courses.dp.ua/ort/ajax/get_data.php", true);
34    XHR.send();
35  };
36 </script>
37 <style> body{ width:800px; margin:0 auto; padding: 10px; } </style></head>
38 <body>
39   <div>Ваше сообщение: <input type="text" id="sms"> <input id="send_btn" type="button" value="Отправить"></div>
40   <hr />
41   <div id="messages"></div>
42 </body></html>
```

*async\_chat.html*

# Реальный

чат



*Час работает с заготовленным API.*

**Интерфейс программирования приложений** (англ. **application programming interface, API**) — набор готовых классов, процедур, функций, структур и констант, предоставляемых приложением (библиотекой, сервисом) для использования во внешних программных продуктах.



# API реального

## чата

[web.dev.courses.dp.ua/ort/ajax/get\\_data.php](http://web.dev.courses.dp.ua/ort/ajax/get_data.php)

Возвращает текстовую HTML разметку содержащую 20 последних сообщений в чате (отсоритрованные по новизне) в приведенном формате:

```
<p> <b> #Номер_сообщения </b> Текст сообщения </p>  
<p> <b> #56 </b> Привет всем!!! </p>
```

### Исходный

```
1 <?php  
2     header('Content-Type: text/html; charset=utf-8');  
3     header('Access-Control-Allow-Origin: *');  
4  
5     mysql_connect('localhost', 'root', '');  
6     mysql_select_db('courses_chat_db');  
7  
8     $result = mysql_query("SELECT * FROM `messages_table` ORDER BY `id` DESC LIMIT 20");  
9  
10    while($one_message = mysql_fetch_array($result)){  
11        ?>  
12        <p>  
13            <b>#<?php echo $one_message['id']; ?></b>  
14            <?php echo $one_message['message_text']; ?>  
15        </p>  
16    <?php } ?>
```

# API реального

## чата

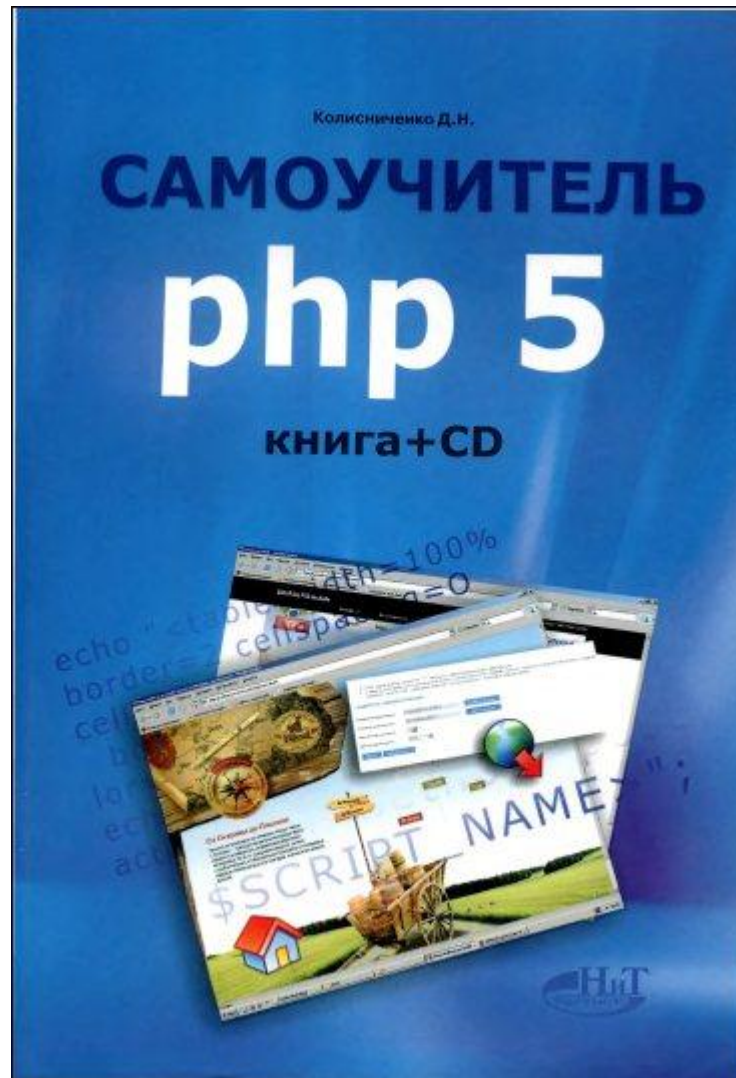
[web.dev.courses.dp.ua/ort/ajax/add\\_data.php](http://web.dev.courses.dp.ua/ort/ajax/add_data.php)

Принимает новое сообщение в чат и заносит его в базу данных, имя принимаемого параметра 'sms' метод передачи параметра GET и POST. В случае успешного добавления возвращается текст 'OK'.

### Исходный

код:

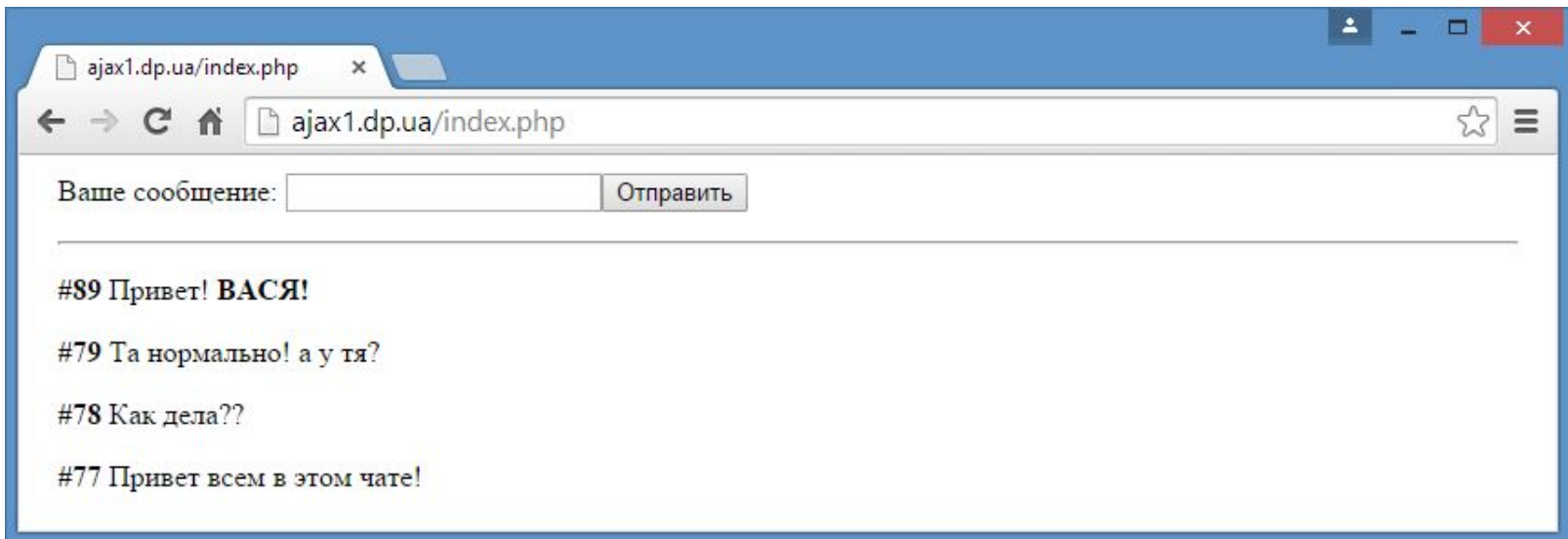
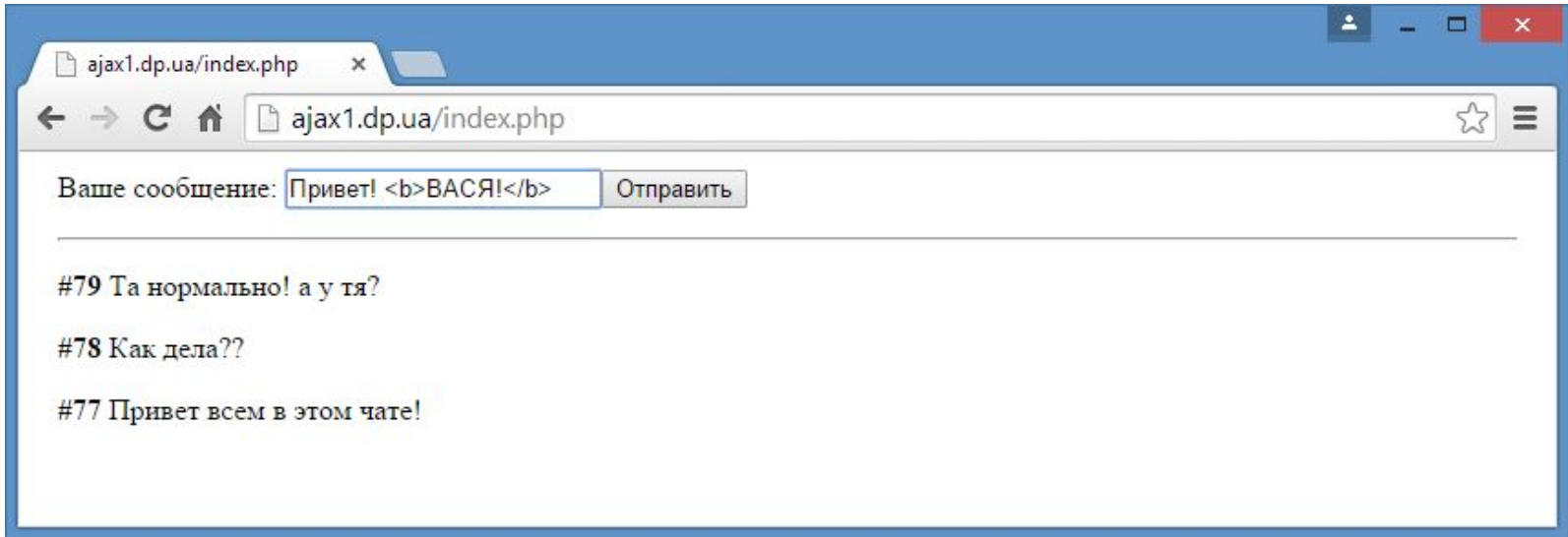
```
1 <?php
2     mysql_connect('localhost', '', '');
3     mysql_select_db('courses_chat_db');
4
5     if(strlen($_REQUEST['sms']) > 1){
6         $sms = mysql_real_escape_string($_REQUEST["sms"]);
7         mysql_query("INSERT INTO `messages_table` (`message_text`) VALUES ('$sms')");
8     }
9
10    header('Content-Type: text/html; charset=utf-8');
11    header('Access-Control-Allow-Origin: *');
12
13    echo "ok";
14 ?>
```



**PHP и MySQL. Разработка Web-  
приложений.**  
*Денис Колисниченко*

Безопасность

# Инъекции кода – Code

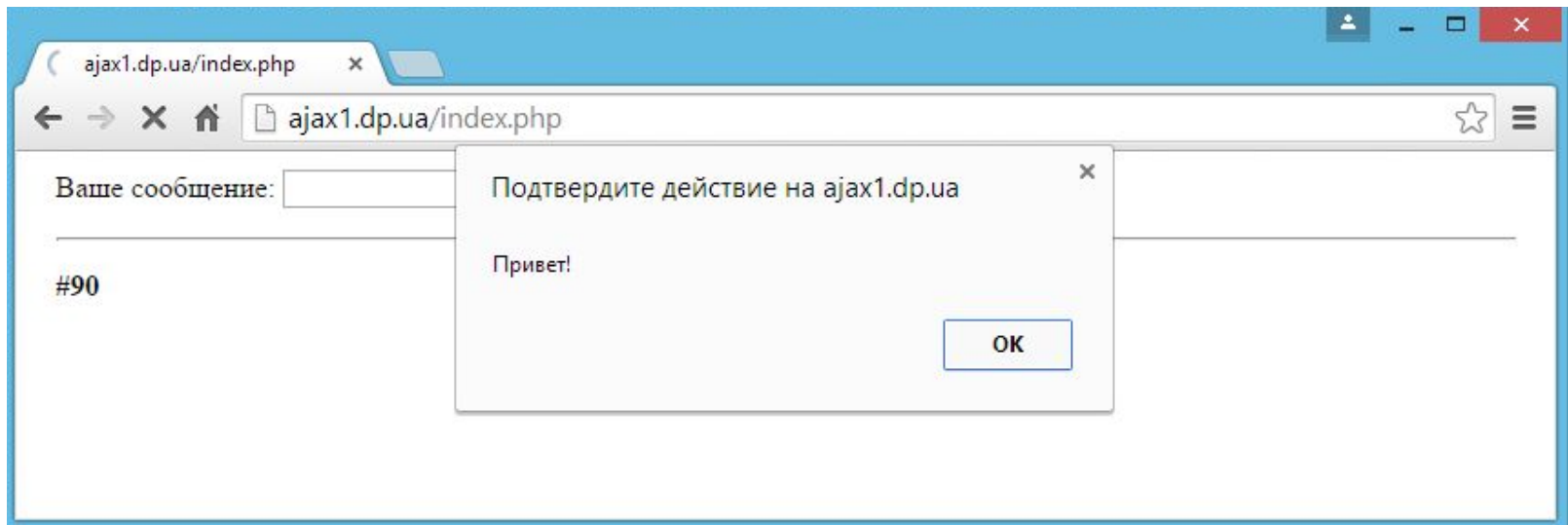
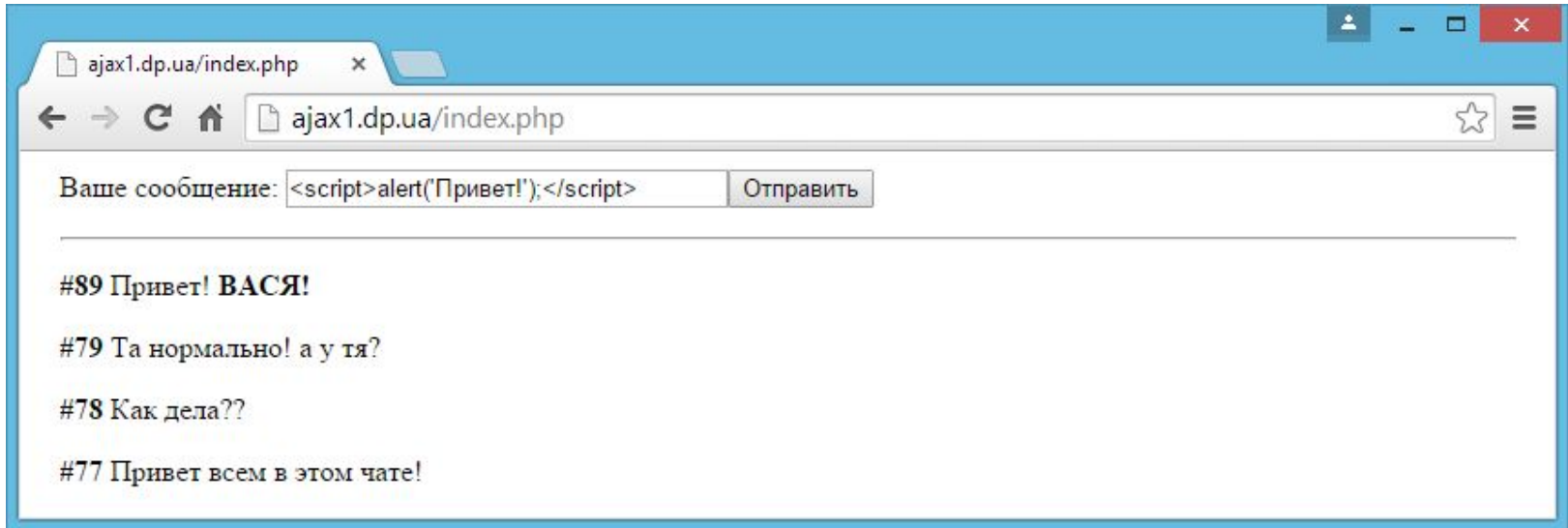


# Инъекции кода – Code injection

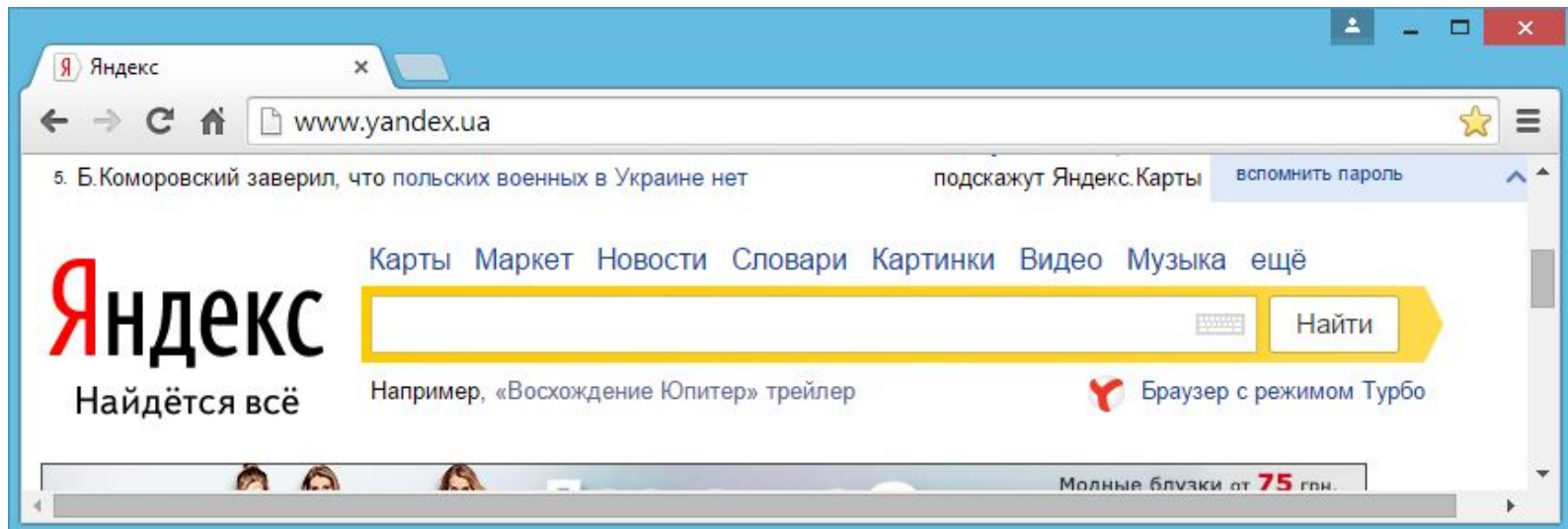
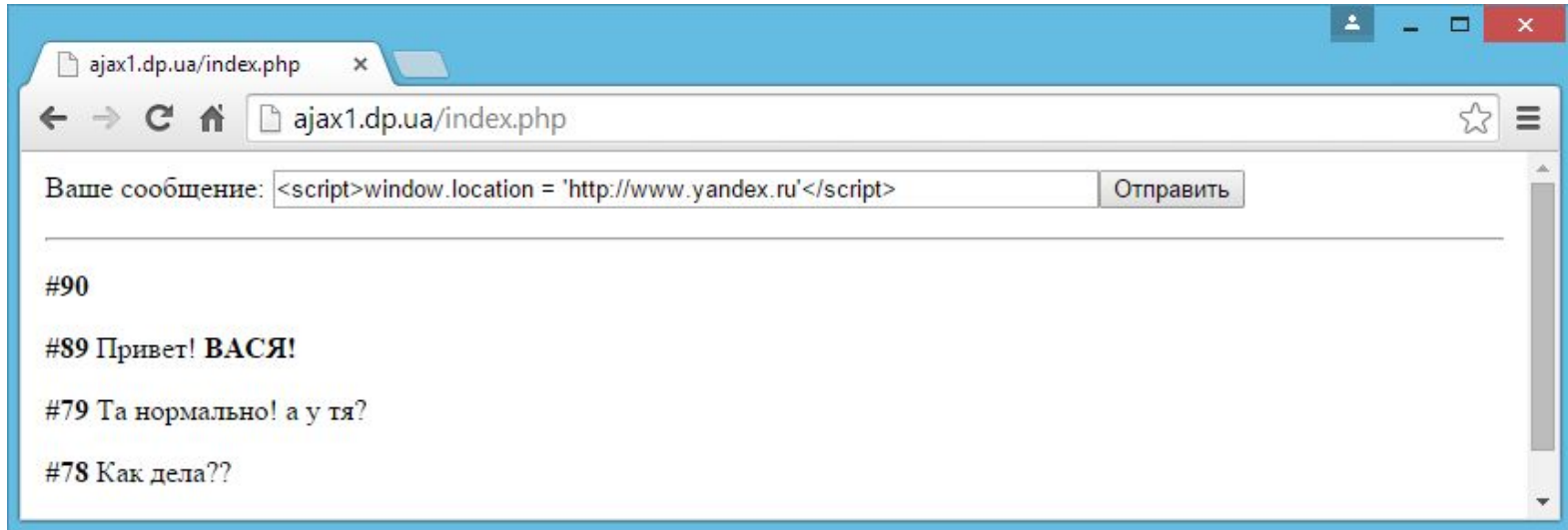


```
1 <html><head>
2
3 <style> body{ width:800px; margin:0 auto; padding: 10px; } </style></head>
4 <body>
5     <form>
6         Ваше сообщение: <input type="text" name="sms"><input type="submit">
7     </form>
8     <hr />
9     <div id="messages">
10         <p>
11             <b>#89</b> Привет! <b>ВАСЯ!</b> </p>
12         <p>
13             <b>#79</b> Та нормально! а у тя? </p>
14         <p>
15             <b>#78</b> Как дела?? </p>
16         <p>
17             <b>#77</b> Привет всем в этом чате! </p>
18     </div>
19 </body></html>
```

# Инъекции кода – Code



# Инъекции кода – Code





# Иньекции кода – Code injection

## Какая защита?

```
<script>alert('Hi!');</script>
```

**php** htmlspecialchars()

```
&lt;script&gt;alert('Привет!');&lt;/script&gt;
```

24  
25  
26  
27

```
<p>  
    <b>#<?php echo $one_message['id']; ?></b>  
    <?php echo htmlspecialchars($one_message['message_text']); ?>  
</p>
```

Ваше сообщение:

Отправить

#91 <script>>window.location = 'http://www.yandex.ru'</script>

#90 <script>alert('Привет!');</script>

#89 Привет! <b>ВАСЯ!</b>

#79 Та нормально! а у тя?

#78 Как дела??

#77 Привет всем в этом чате!

# Ињекција SQL – SQL

```
injection  
$sms = $_REQUEST["sms"];  
$query = "INSERT INTO `messages_table` (`message_text`) VALUES ('$sms')"
```

Ваше сообщение:

Отправить



```
"INSERT INTO `messages_table` (`message_text`) VALUES ('xx')); DROP TABLE  
messages_table; -- ')"
```

## Какая

```
5  if(strlen($_REQUEST['sms']) > 1){  
6     $sms = mysql_real_escape_string($_REQUEST["sms"]);  
7     mysql_query("INSERT INTO `messages_table` (`message_text`) VALUES ('$sms')");  
8     header('Location: ./index.php');  
9 }
```

**xx')**; DROP TABLE messages\_table; --



**xx\')**; DROP TABLE messages\_table; --

# Cookie/Сессии/Параметры в URL

На стороне клиента можно хранить только его

The screenshot shows the Rozetka website in the Opera browser. The page includes a search bar, navigation links, and category buttons. The developer tools are open to the 'Resources' tab, displaying a table of cookies.

Name	Value	Domain	Path	Expires / ...	Size	HTTP	Secure
__utma	28000675.866512184.1412923868.1421526300.142201...	.rozetka...	/	2017-01...	60		
__utmb	28000675.1.10.1422013404	.rozetka...	/	2015-01...	30		
__utmc	28000675	.rozetka...	/	Session	14		
__utmz	28000675.1421526300.10.6.utmcsrc=google utmccn=(or...	.rozetka...	/	2015-07...	100		
_dc_gtm_UA-203518-6	1	.rozetka...	/	2015-01...	20		
_ga	GA1.3.866512184.1412923868	.rozetka...	/	2017-01...	29		
ab_search_abtests_id	10	.rozetka...	/	2015-04...	22		
cid	AqyQIQ5F7giegpA82Dc7K8A	.adriver.ru	/	2029-12...	26		
device_type	computer	.rozetka...	/	2015-10...	19		
href	http%3A%2F%2Frozetka.com.ua%2F	.rozetka...	/	2015-01...	34		
partner_id	1	.rozetka...	/	2015-03...	11		
sessionSource	google/organic utmctr=(not%20provided)	.rozetka...	/	2015-07...	51		
uid	WbhRg156xRouN1hEAXDeAg==	.rozetka...	/	2015-01...	27		