

**УЛЬЯНОВСКИЙ ГОСУДАРСТВЕННЫЙ
УНИВЕРСИТЕТ**

Факультет математики, информационных и авиационных
технологий

НАУЧНО-ИССЛЕДОВАТЕЛЬСКАЯ РАБОТА

**НА ТЕМУ:
«РАЗРАБОТКА МОДУЛЯ АУТЕНТИФИКАЦИИ
ВЕБ-РЕСУРСОВ ПРЕДПРИЯТИЯ»»**

Выполнил студент 6 курса

Е.И. Шабров

Научный руководитель

А.М Иванцов

Ульяновск - 2022

Цели и задачи работы

- Цель научно-исследовательской работы – разработка модуля аутентификации веб-ресурсов предприятия.
- Задачи, реализующие цель работы:
 1. Провести анализ угроз веб-ресурсам.
 2. Выявить требования к защите веб-ресурсов.
 3. Проанализировать способы и криптографические протоколы аутентификации.
 4. Выявить основные угрозы безопасности при аутентификации.
 5. Разработать и обосновать структуру криптографического модуля веб-приложения предприятия – ее функционал и алгоритм работы.
 6. Осуществить программную реализацию криптографического модуля веб-приложения предприятия.



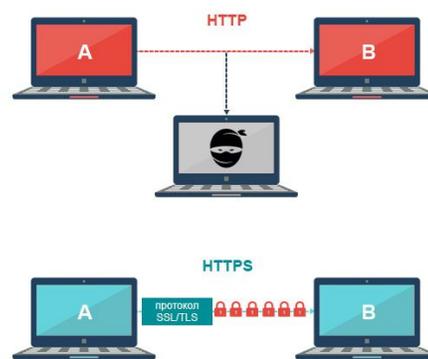
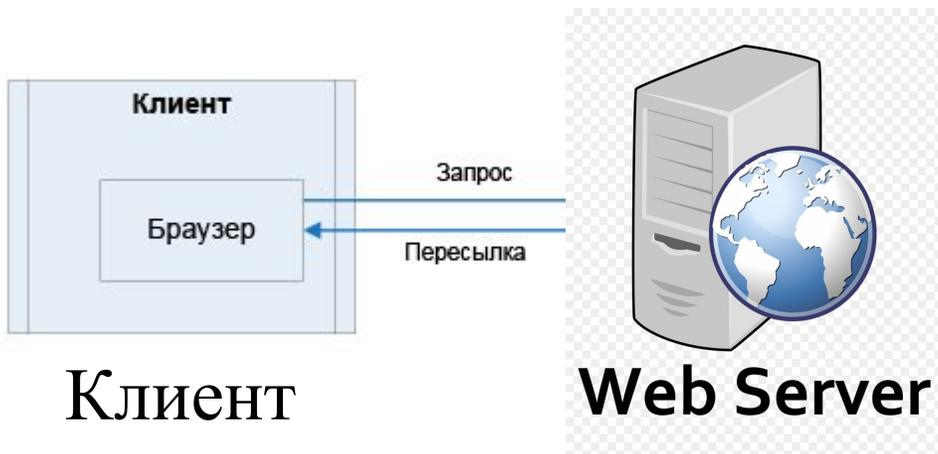
Понятие о веб-ресурсе

Веб-ресурс это:

Одна или несколько логически связанных между собой веб-страниц; также место расположения контента сервера



IP-адрес

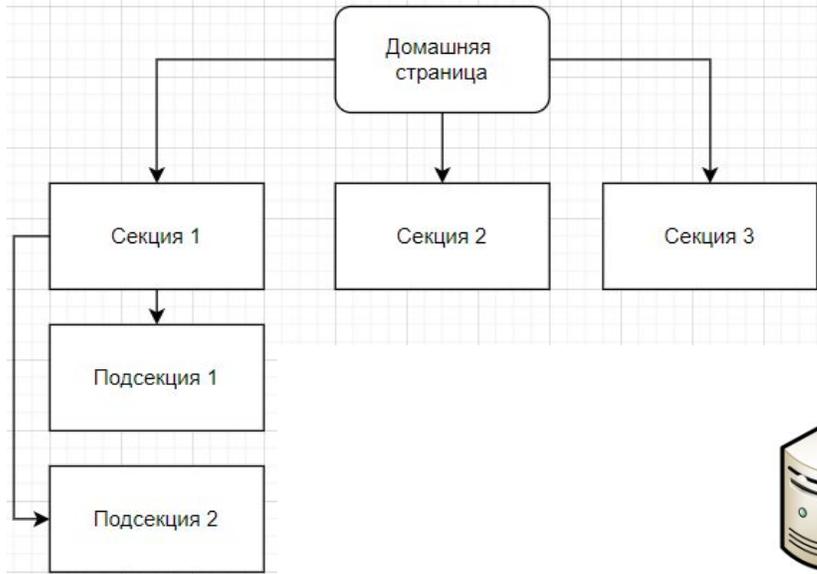


Протокол

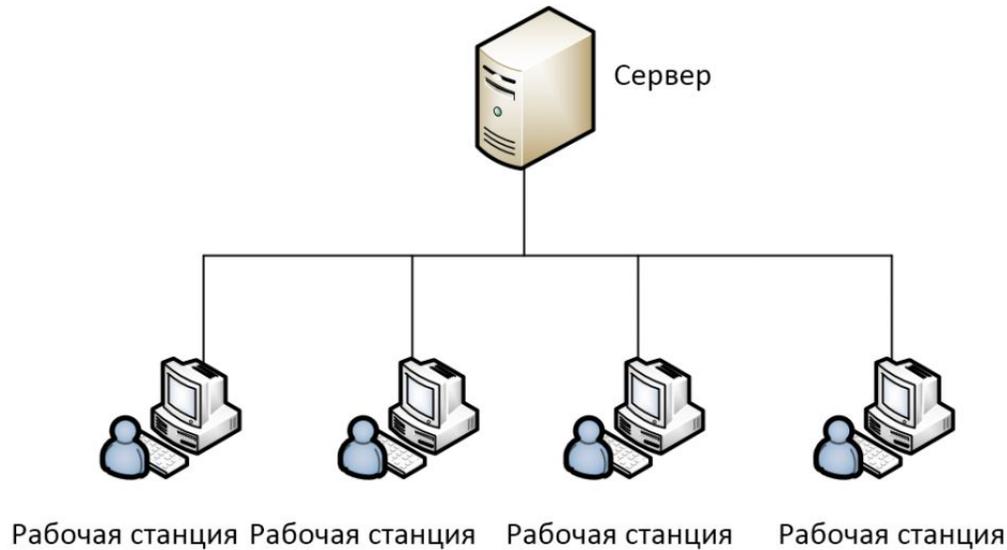


Авторизация и аутентификация

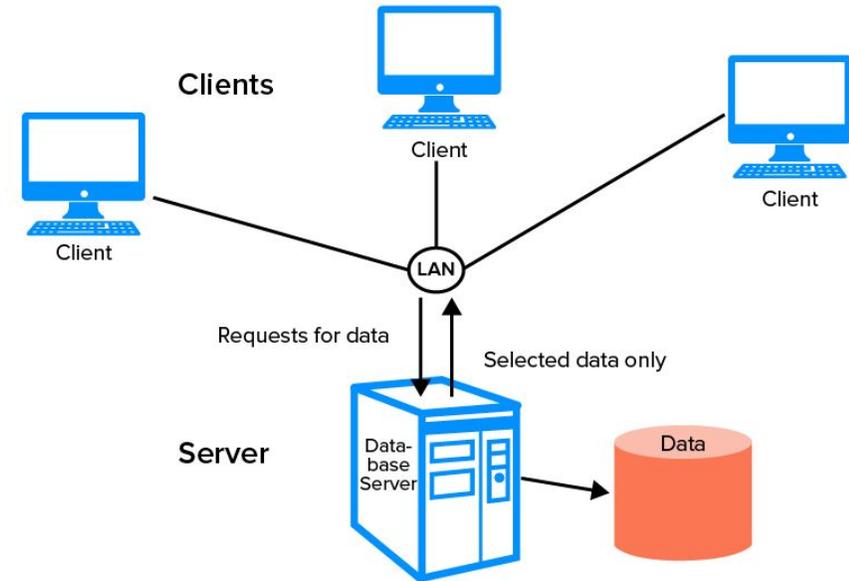
Структура клиентской части веб-ресурса



Процедура взаимодействия клиент-сервер



Client/ Server Architecture



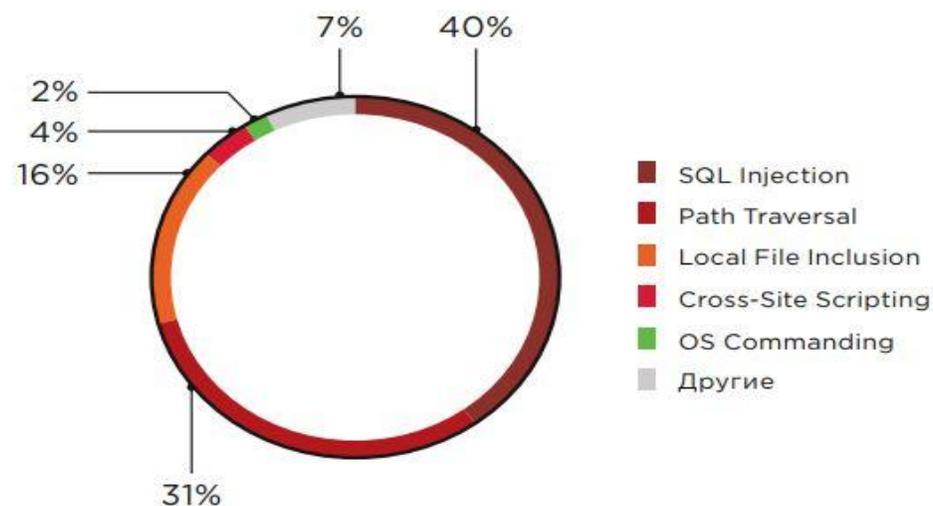
Основные угрозы для веб-ресурсов предприятия

Основные типы угроз информационной безопасности веб-приложения :

- Угрозы конфиденциальности – несанкционированный доступ к данным.
- Угрозы целостности – несанкционированное искажение или уничтожение данных.
- Угрозы доступности – ограничение или блокирование доступа к данным.

Тройка наиболее распространенных атак на веб-ресурсы не меняется из года в год:

1. «Внедрение SQL-кода»
2. «Выход за пределы каталога»
3. «Межсайтовое выполнение сценариев»



Основные требования к защите веб-ресурсов

Требования	Документ
<ul style="list-style-type: none"> Разработка на основе модели угроз системы защиты информации, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты информации. 	Приказ от 31 августа 2010 года N 489 [13]
<ul style="list-style-type: none"> Модификация сайта должна быть возможна за кратчайшие сроки. Необходимо использовать протоколы безопасности при передаче данных между локальным компьютером и сервером. Должна проводиться регулярная проверка файлов журнала доступа и ошибок сервера (log-файлы) на предмет несанкционированного доступа. Должна проводиться проверка подлинность идентификации осуществлять аутентификацию Управлять обновлениями программного обеспечения 	Технические требования по обеспечению безопасности веб-ресурсов [14]
<ul style="list-style-type: none"> Безопасность персональных данных при их обработке в информационной системе обеспечивается с помощью системы защиты персональных данных, нейтрализующей актуальные угрозы. 	Постановление Правительства РФ от 01.11.2012 N 1119 "Об утверждении требований к защите персональных данных при их обработке в

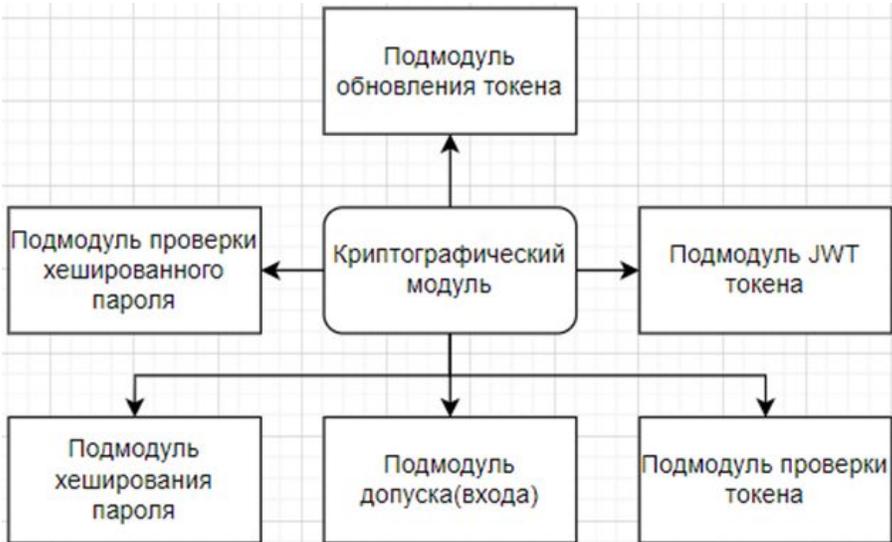
	информационных системах персональных данных" [9]
<ul style="list-style-type: none"> Все криптографические протоколы должны реализовывать в среде специальных аппаратных средств СКЗИ Для каждого конкретного средства регистрации должны проводиться работы по оценке влияния данной модели на выполнение СКЗИ предъявляемых требований Специальные аппаратные средства СКЗИ должны реализовывать в себе совокупность аппаратно-программных систем защиты В СКЗИ должен быть реализован форматно-логический контроль информации 	Выписка «Требования к средствам криптографической защиты информации, предназначенным для обеспечения некорректируемой регистрации информации, не содержащей сведений, составляющих государственную тайну» ФСБ России от 23.09.2019
<ul style="list-style-type: none"> Идентификация и аутентификация включают в себя распознавание пользователя средств доверенной третьей стороны, члена группы администраторов средств или процесса и проверку их подлинности. Механизм аутентификации должен блокировать доступ этих субъектов к функциям средств ДТС при отрицательном результате аутентификации. 	Приказ ФСБ России от 04.12.2020 N 556 (ред. От 13.04.2021) [25]

Основные способы аутентификации веб-ресурсов

Способ	Основное применение	Протоколы	По электронной подписи	Аутентификация пользователей	Протокол ССІТТ X.509, Транспортный протокол Шампра
По паролю	Аутентификация пользователей	HTTP, Forms	По биометрическим данным	Аутентификация пользователей в безопасных приложениях	Протоколы РАКЕ, ВАКЕ
По одноразовым паролям	Дополнительная аутентификация пользователей (для достижения two-factor authentication)	Forms	По GPS	Аутентификация пользователей	Протокол NTRIP
По ключам доступа	Аутентификация сервисов и приложений	-			
По токенам	Делегированная аутентификация пользователей; делегированная авторизация приложений	SAML, WS-Federation, OAuth, OpenID Connect			
По сертификатам	Аутентификация пользователей в безопасных приложениях; аутентификация сервисов	SSL/TLS			

Криптографического модуль защиты веб-ресурсов предприятия

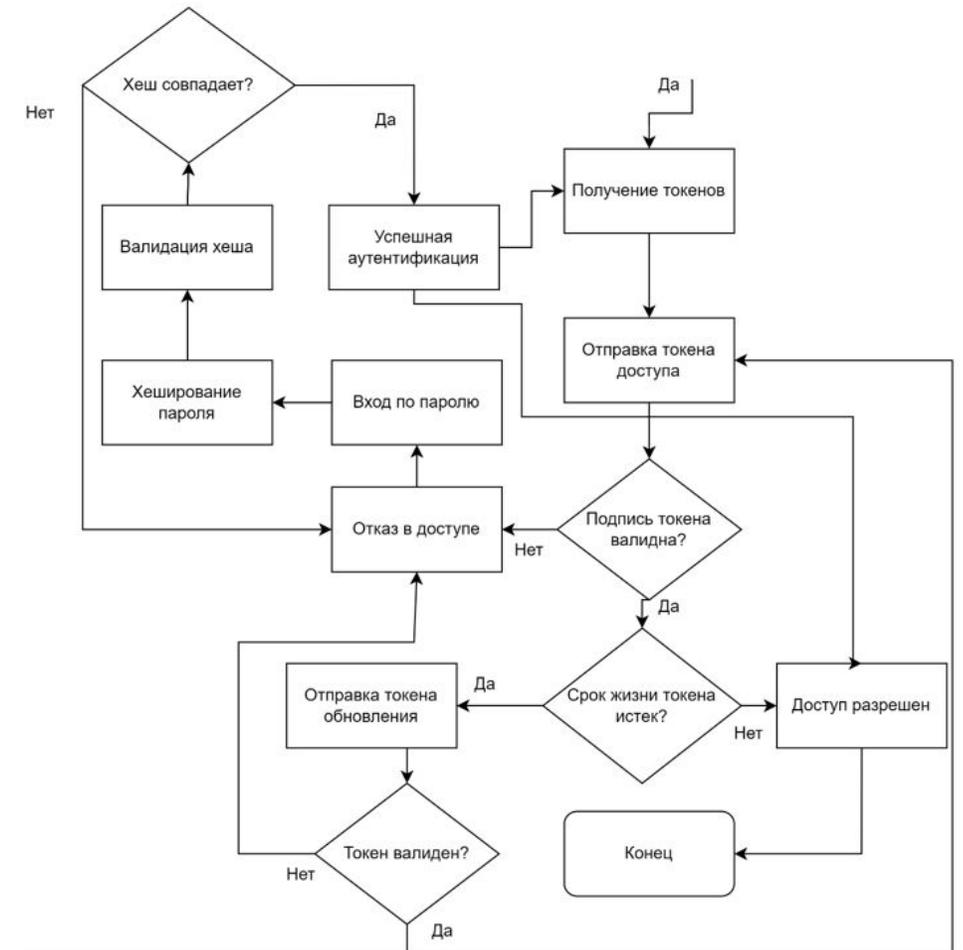
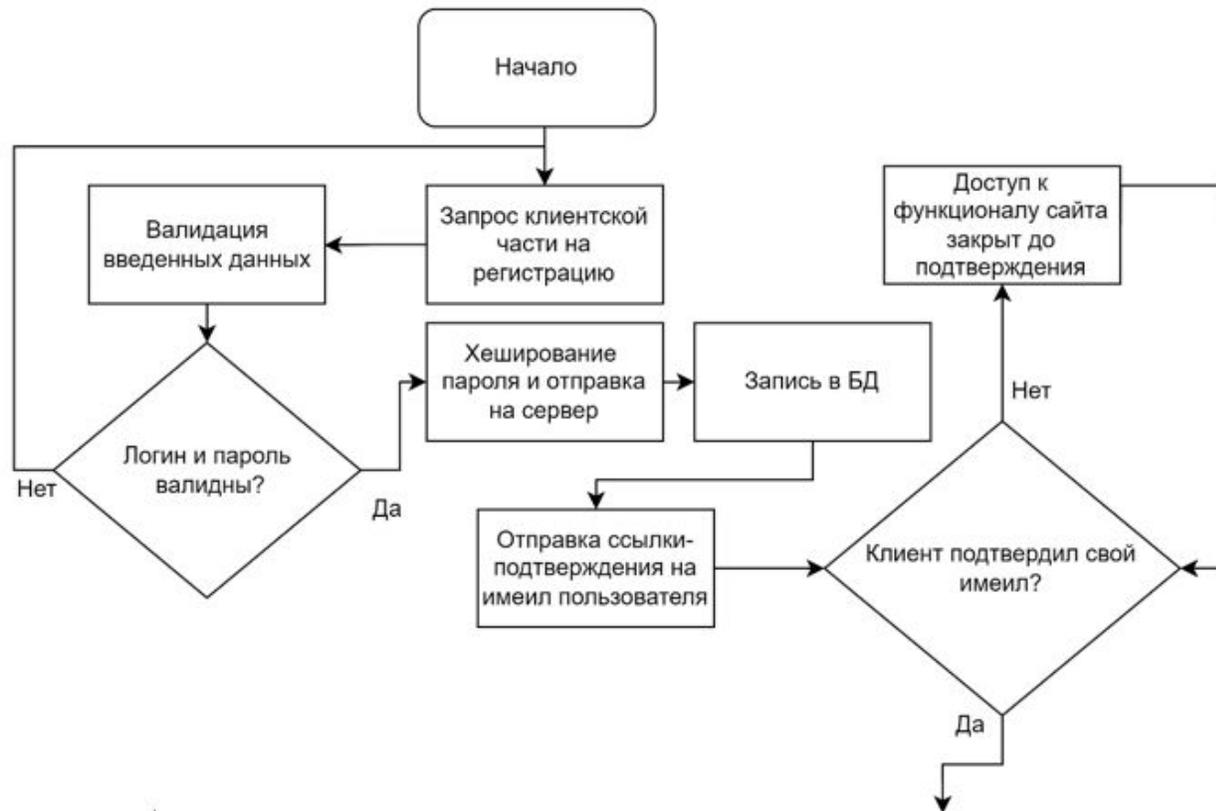
Структуре криптографического модуля



В основной состав криптографического модуля веб-приложения предприятия входят такие элементы как:

- Подмодуль хеширования пароля
- Подмодуль валидации хешированного пароля
- Подмодуль допуска
- Подмодуль JWT токена
- Подмодуль проверки токена
- Подмодуль обновления токена

Алгоритм работы криптографического модуля веб-ресурса предприятия



Пример работы программы

С начала происходит вход пользователем на стартовую страницу

The first screenshot shows a green login form titled 'Вход' with two input fields: 'Email' and 'Пароль'. Below the fields are two buttons: 'Логин' and 'Регистрация'. The second screenshot shows the same form with the email field containing 'coolmenclash@yandex.ru' and the password field containing a masked password. The buttons remain the same.

В случае если данные не проходят валидацию на сервере, выводится ошибка:

The third screenshot shows the login form with the email field containing 'фывфыв' and the password field masked with dots. The buttons 'Логин' and 'Регистрация' are still present. To the right of the form, a dark sidebar contains a list of items under the heading 'Name'. The first item is 'login' with a checked checkbox, and the following six items are 'registration' with unchecked checkboxes.

После регистрации и успешного пройденного теста на валидацию пароля и логина, пароль хешируется функцией стрибог и заносится в БД, вот как это выглядит:

```
_id: ObjectId("631c94c2c2148c45aef64bf4")
email: "sshabrovivivi@gmail.com"
password: "d##$n#d6Fc/cPEf.#eW0D$94mD1d#$y##2lwN7/./5/$I.AF53V0U$03$.m2o.$"
isActivated: false
```

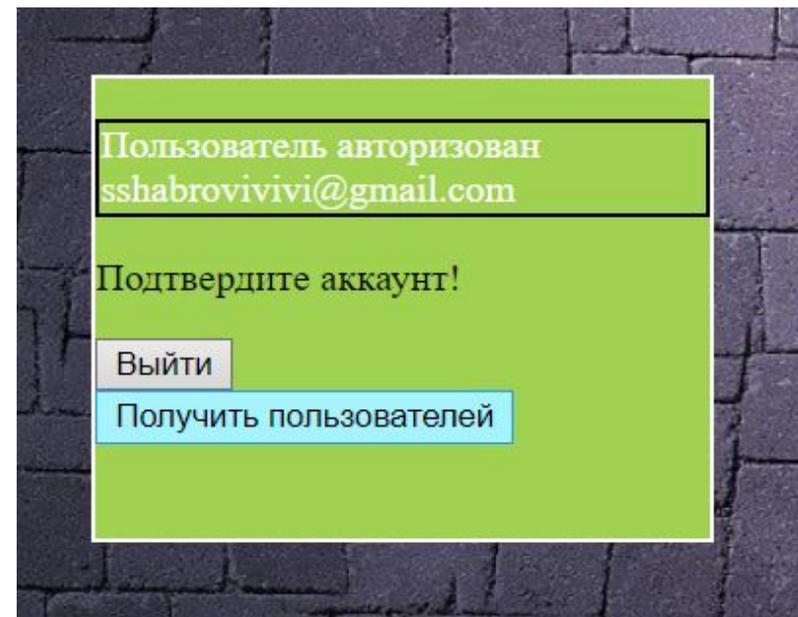
После входа пользователя пускает на сервер, но функциями веб-ресурса он пользоваться не может. Здесь в качестве демонстрации таких функций присутствует кнопка «получить пользователей». Поскольку пользователь не подтвердил свой аккаунт, не перейдя по ссылке активации, отправленной ему на имеил

Активация аккаунта на <http://localhost:5000>

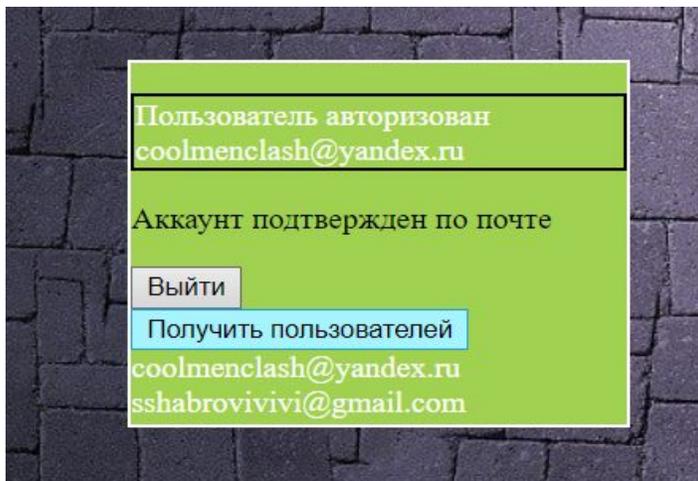
 coolmenclash@yandex.ru coolmenclash@yandex.ru  Сегодня в 16:04
Я >

Для активации перейдите на ссылке

<http://localhost:5000/api/activate/f2cbea69-0568-49bc-97da-850e261ff82b>



После подтверждения аккаунта можно пользоваться функциями ресурса, причем функции могут находиться на стороннем сервере, пользователь все равно сможет ими пользоваться из-за наличия в куки токена доступа:



Также возможно возникновение ошибок, связанных с невнимательностью самого пользователя во время входа в аккаунт, таких как:

```
Server started on 5000
ApiError: Пользователь с почтовым адресом coolmenclash@yandex.ru уже существует
```

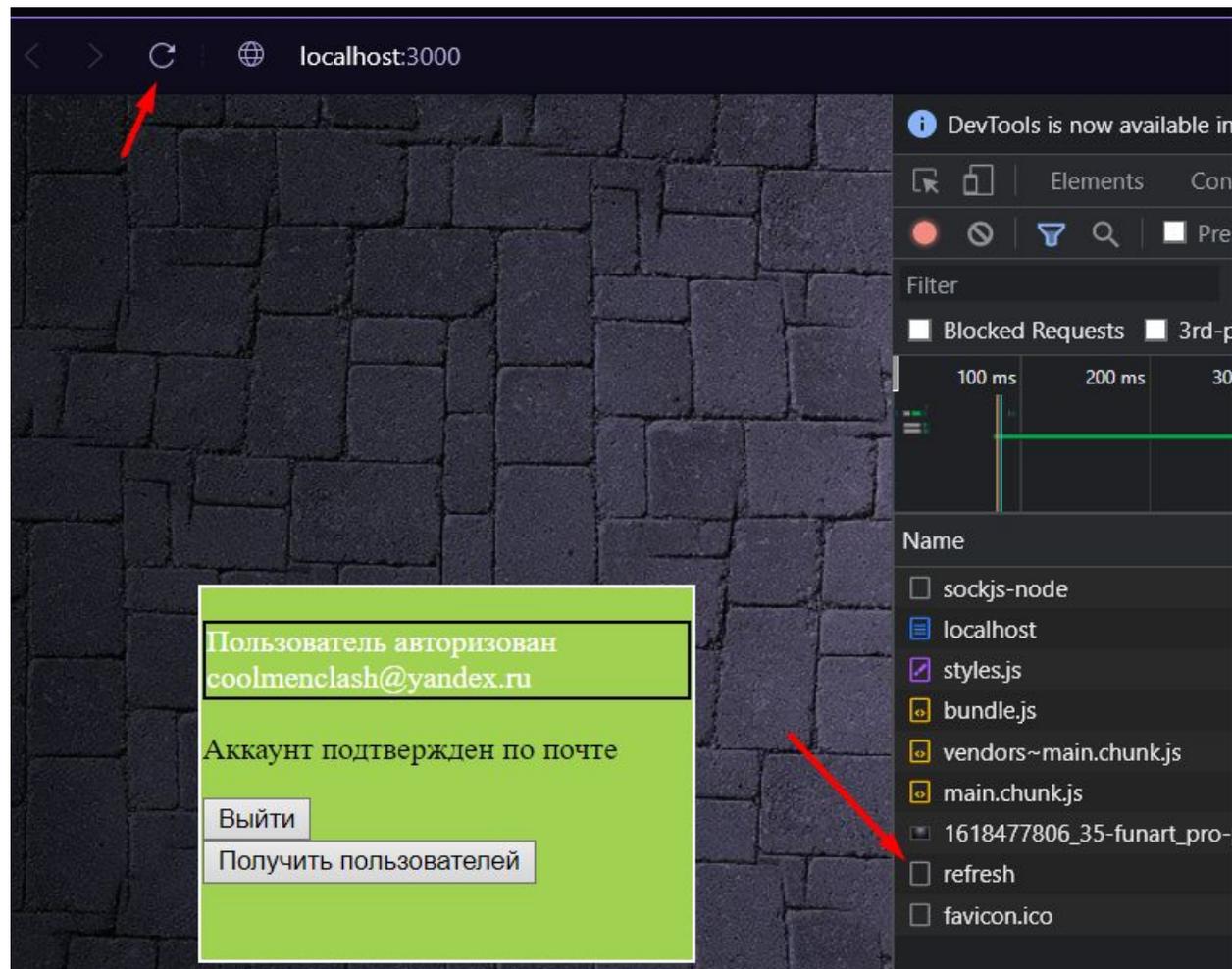
Активация аккаунта также прописывается в БД:

QUERY RESULTS: 1-2 OF 2

```
_id: ObjectId("631c7d48ec46d6fe855004fb")
email: "coolmenclash@yandex.ru"
password: "d##$n#d6Fc/cPEf.#eW0D$94mD1d##$y##2lwN7/. /5/$I.AF53V0U$03$.m2o.$"
isActive: true
activationLink: "f2cbea69-0568-49bc-97da-850e261ff82b"
__v: 0
```

```
_id: ObjectId("631c94c2c2148c45aef64bf4")
email: "sshabrovivivi@gmail.com"
password: "d##$n#d6Fc/cPEf.#eW0D$94mD1d##$y##2lwN7/. /5/$I.AF53V0U$03$.m2o.$"
isActive: false
```

При обновлении страницы, в случае если токен доступа истек, клиент отправляет токен обновления, его отправку можно увидеть в панели разработчика:



Еще один пример обращения к функции ресурса при истекшем токене доступа (пункт user) и немедленная отправка токена обновления (refresh):

<input type="checkbox"/>	users	200	xhr	xhr.js:...	26...	11...
<input type="checkbox"/>	users	401	xhr	xhr.js:...	40...	5 ...
<input type="checkbox"/>	refresh	200	xhr	xhr.js:...	1...	41...
<input type="checkbox"/>	users	200	xhr	xhr.js:...	26...	14...

Представление токенов в куки клиента:

```
"accessToken": "eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1IjoiSm1tIiwiaWF0IjoxNTY4NzU4MTg0LCJleHAiOjE1Njg3NTg0OT19.uWF4goP2qKLv4bbJB2b2Ebmzu8NAkII4FB7d0qjElzY",
  "refreshToken": "eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1IjoiSm1tIiwiaWF0IjoxNTY4NzU4MTg0fQ.Jjv1aQsSgmVRc3E7i1rXC15usKq8DMcSzxFEMj__0p4"
}
```

Спасибо за внимание!

