

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ

Федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский университет ИТМО»

Информационная безопасность

Работа 7: Безопасность браузера и анализ сетевого трафика

Выполнил:

Румский Александр Максимович

Группа:

Р3407

Преподаватель:

Маркина Татьяна Анатольевна

Санкт-Петербург, 2025 год

Содержание

| | |
|---|----|
| Настройка браузера | 3 |
| Выбор уровня защиты | 3 |
| Настройки конфиденциальности и сохранение куки..... | 4 |
| Настройки сохранения паролей..... | 4 |
| История | 5 |
| Доступ к аудио/видео устройствам и геолокации | 5 |
| Сбор аналитических данных браузером..... | 6 |
| Защита на сайтах | 7 |
| Анализ трафика | 9 |
| Запрос | 9 |
| Ответ..... | 10 |
| Формат отправки данных пользователя | 11 |
| Ответ на вопрос | 12 |

Настройка браузера

Выбор уровня защиты

Приватность браузера

Улучшенная защита от отслеживания



Трекеры отслеживают вас в Интернете, чтобы собирать сведения о ваших привычках и интересах. Firefox блокирует многие из этих трекеров и других вредоносных скриптов.

[Подробнее](#)

[Управление исключениями...](#)

☐ Стандартная

Золотая середина: защита и производительность. Страницы будут загружаться нормально.

☒ Строгая

Усиленная защита может вызывать проблемы с некоторыми сайтами и их содержимым.

Firefox блокирует следующее:

- Трекеры соцсетей
- Межсайтовые куки во всех окнах
- Отслеживающее содержимое во всех окнах
- Криптомайнеры
- Известные и предполагаемые сборщики цифровых отпечатков

☒ Устранение основных проблем с сайтами (рекомендуется)

Помогает загружать сайты и функции, разблокируя только необходимые элементы, которые могут содержать трекеры. Покрывает наиболее распространенные проблемы. [Подробнее](#)

☒ Устранение незначительных проблем с сайтами

Восстанавливает такие вещи, как видео в статье или комментарии, разблокируя элементы, которые могут содержать трекеры. Это может уменьшить проблемы с сайтом, но даст более слабую защиту. Должен использоваться с исправлениями для основных проблем.

Некоторые сайты могут не работать со строгой защитой от отслеживания

Firefox рекомендует использовать настройки «Устранение проблем с сайтом», чтобы уменьшить количество неработоспособных сайтов и содержимого. Если сайт кажется неработающим, попробуйте отключить защиту от отслеживания на этом сайте, чтобы загрузить всё содержимое. [Подробнее](#)

☐ Персональная


Выберите, какие трекеры и скрипты необходимо блокировать.

Настройки конфиденциальности и сохранение куки

Настройки конфиденциальности веб-сайта

☒ Сообщать веб-сайтам, чтобы они не продавали и не разглашали мои данные [Подробнее](#)

Куки и данные сайтов

 Удалить данные веб-сёрфинга (Ш) >

Ваши сохранённые куки, история, данные сайтов и кеш сейчас занимают на диске **0 байт**.

Управление данными веб-сёрфинга (Ь) >

Управление исключениями
Вы можете указать, каким веб-сайтам всегда разрешено или никогда не разрешено использовать куки и данные сайта. >

☒ Удалять куки и данные сайтов при закрытии Firefox

Настройки сохранения паролей

Пароли

☐ Просить сохранить пароли (Ф)

Исключения...

☒ Автоматически заполнять имена пользователей и пароли

Сохранённые пароли (В)

☒ Предлагать надёжные пароли

☒ Предлагать псевдонимы электронной почты Firefox Relay для защиты вашего адреса электронной почты [Подробнее](#)

☒ Показывать уведомления о паролях для взломанных сайтов [Подробнее](#)

☐ Требовать вход на устройстве для заполнения и управления паролями

☐ Использовать основной пароль [Подробнее](#)

Изменить основной пароль...

Ранее — мастер-пароль

☐ Разрешить единый вход Windows для учётных записей Microsoft, учётных записей на работе и в учебных заведениях [Подробнее](#)

Управление аккаунтами в настройках вашего устройства

[Управление ключами доступа в системных настройках](#)

История

История

Firefox будет использовать ваши настройки хранения истории ▾

☐ Всегда работать в приватном режиме Удалить историю...


☒ Помнить историю посещений и загрузок


☒ Помнить историю поиска и данных форм


☒ Удалять историю при закрытии Firefox Параметры...


Доступ к аудио/видео устройствам и геолокации


Разрешения


 Местоположение Параметры...


 Камера Параметры...

 Микрофон Параметры...

 Выбор динамика Параметры...

 Уведомления [Подробнее](#) Параметры...

 Автовоспроизведение Параметры...

 Виртуальная реальность Параметры...

☒ Блокировать всплывающие окна и сторонние перенаправления Исключения...

☒ Предупреждать при попытке сайтов установить дополнения Исключения...


Сбор аналитических данных браузером

Сбор и использование данных Firefox

Мы стремимся предоставить вам возможность выбора и собираем только минимальные данные, необходимые для улучшения Firefox для всех и каждого.

[Просмотреть Уведомление о конфиденциальности](#)

Эти настройки применяются ко всем профилям Firefox на этом устройстве. [Просмотреть все профили](#)

 Вы больше не разрешаете Mozilla собирать технические данные и данные взаимодействия. Все собранные ранее данные будут удалены в течение 30 дней. [Подробнее](#)

☐ Отправлять технические данные и данные взаимодействия в Mozilla

Это поможет нам улучшить возможности, производительность и стабильность Firefox. [Подробнее](#)

☐ Разрешить персонализированные рекомендации расширений

Получать рекомендации расширений, чтобы улучшить свою работу в Интернете. [Подробнее](#)

☐ Установка и запуск исследований

Опробуйте функции и идеи перед тем, как они станут доступны для всех и каждого.

[Просмотреть исследования Firefox](#)

☐ Отправлять ежедневный пинг использования в Mozilla

Это помогает Mozilla оценить активных пользователей. [Подробнее](#)

☐ Автоматически отправлять сообщения о падениях

Это помогает Mozilla диагностировать и устранять проблемы с браузером. Отчёты могут содержать личные или важные данные. [Подробнее](#)

Защита на сайтах

Защита

Поддельное содержимое и защита от вредоносных приложений

- ☒ Блокировать опасное и обманывающее содержимое [Подробнее](#)
 - ☒ Блокировать опасные загрузки
 - ☒ Предупреждать о нежелательных и редко загружаемых приложениях

Сертификаты

Настроить сертификаты, которые Firefox использует для аутентификации. [Подробнее](#)

Просмотр сертификатов...



Устройства защиты...



- ☒ Разрешить Firefox автоматически доверять установленным вами сторонним корневым сертификатам. [Подробнее](#)

Режим «Только HTTPS»

Разрешает только защищённые соединения с веб-сайтами. Firefox будет спрашивать перед незащищённым соединением. [Подробнее](#)

- ☒ Включить режим «Только HTTPS» во всех окнах
- ☐ Включить режим «Только HTTPS» только в частных окнах
- ☐ Не включать режим «Только HTTPS»
Firefox сможет всё ещё переключать некоторые соединения [Подробнее](#)

Управление исключениями...



DNS через HTTPS

Система доменных имен (DNS) через HTTPS отправляет ваш запрос на доменное имя через зашифрованное соединение, обеспечивая безопасный DNS и мешая другим увидеть, к какому веб-сайту вы собираетесь получить доступ.

[Подробнее](#)

Состояние: Активно

Поставщик: Cloudflare

Управление исключениями...

Включить DNS через HTTPS, используя:

☐ **Защиту по умолчанию**

Firefox решает, когда использовать безопасный DNS для защиты вашей конфиденциальности.

☐ **Повышенную защиту**

Вы сами решаете, когда использовать безопасный DNS, и выбираете своего поставщика.

☒ **Максимальную защиту**

Firefox всегда будет использовать безопасный DNS. Вы увидите предупреждение об угрозе безопасности, прежде чем мы будем использовать DNS вашей системы.

- Использовать только выбранного вами поставщика
- Всегда предупреждать, если безопасный DNS недоступен
- Если безопасный DNS недоступен, сайты не будут загружаться или работать должным образом.

Выбрать поставщика:

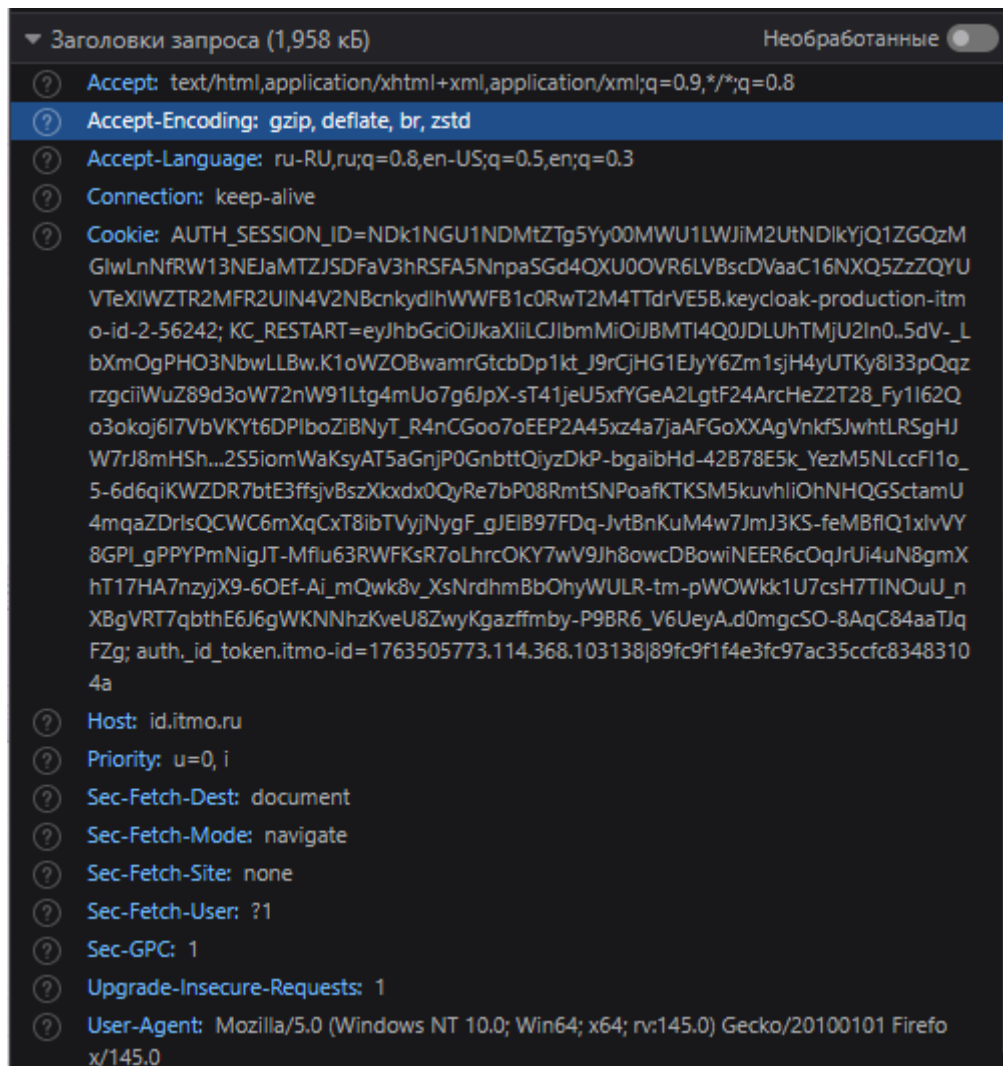
Cloudflare (По умолчанию)

☐ **Отключить**

Использовать разрешение DNS по умолчанию

Анализ трафика

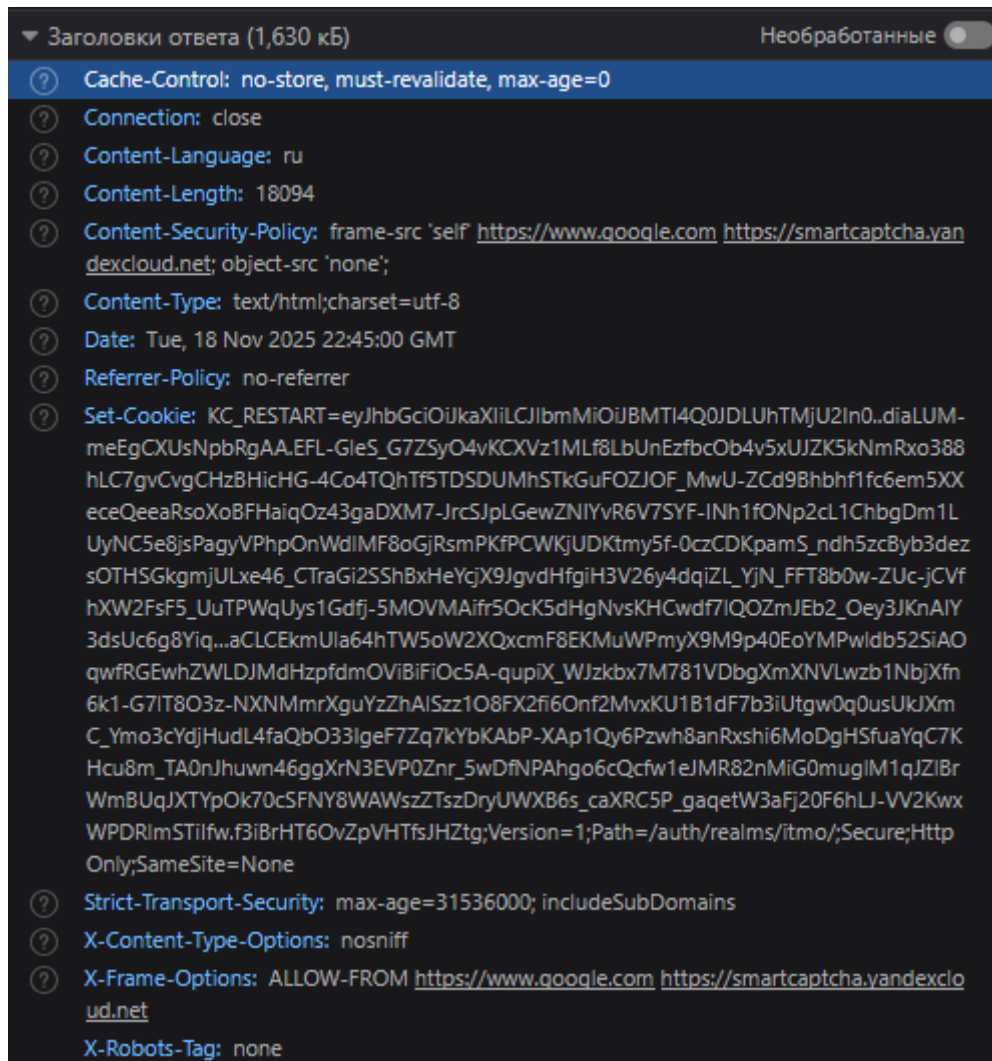
Запрос



Sec-GPC: 1 – из-за настроек браузера, сигнал о желании пользователя не продавать его данные

Upgrade-Insecure-Requests: 1 - из-за настроек браузера, если возможно, заменять HTTP на HTTPS

Ответ



Cache-Control: no-store, must-revalidate, max-age=0 - указывает браузеру и промежуточным кэширующим серверам не хранить копию ответа

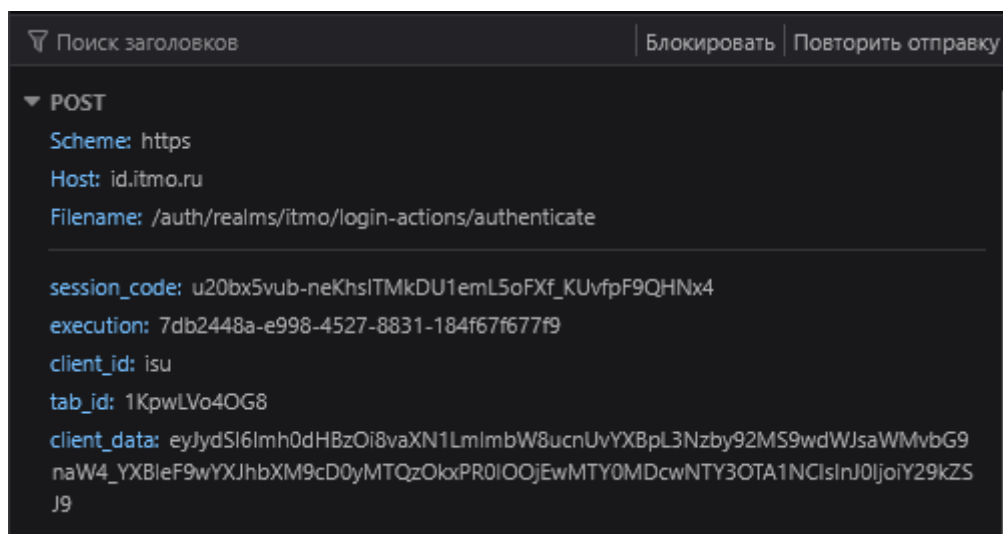
Content-Security-Policy: frame-src 'self' <https://www.google.com> <https://smartcaptcha.yandexcloud.net>; object-src 'none'; - Политика безопасности, ограничивающая, откуда могут загружаться определённые ресурсы, в том числе запрещает загрузку плагинов

X-Content-Type-Options: nosniff - Запрещает браузеру угадывать MIME-тип контента, предотвращая атаки, связанные с неправильной интерпретацией файлов

X-Robots-Tag: none - инструктирует поисковым роботам не индексировать страницу и не переходить по ссылкам на ней

Формат отправки данных пользователя

Вход в ИСУ



Ответ на вопрос

Как чаще всего передаются данные аутентификации (логин/пароль) в современных веб-приложениях?

В современных веб-приложениях логин и пароль чаще всего передаются через форму на странице, отправляемую по HTTPS через POST запрос формы или в формате JSON. Этот метод сочетается с сессионными cookies или JSON Web Tokens (JWT) для поддержания состояния аутентификации.

Альтернатива – сторонние сервисы для аутентификации, когда логин/пароль получает провайдер, а возвращает только токен доступа.