КОМИТЕТ ПО МОЛОДЕЖНОЙ ПОЛИТИКЕ
И ВЗАИМОДЕЙСТВИЮ С ОБЩЕСТВЕННЫМИ
ОРГАНИЗАЦИЯМИ

ЦЕНТР СТУДЕНЧЕСКИХ ИНИЦИАТИВ СЗ СЕВЕРО-ЗАПАД

МЫ!! ПЕТЕРБУРГ

Методический материал «Технологические подходы формирования сообществ в сети «Интернет». Краткое описание»

Санкт-Петербург
2020

Методический материал разработан Комитетом по молодежной политике и взаимодействию с общественными организациями совместно с общественной организацией «Центр студенческих инициатив «Северо-Запад» и автономной некоммерческой организацией разработки и сопровождения инновационных проектов «Центр системных инициатив» в рамках реализации просветительских мероприятий для специалистов по молодёжной политике Санкт-Петербурга в условиях цифровой среды.

Методический материал «Технологические подходы формирования сообществ в сети «Интернет». Краткое описание» адресован специалистам по молодёжной политике Санкт-Петербурга и регионов России, а также всем, кто интересуется вопросами воспитания молодёжи в условиях цифровой среды.

Методический материал посвящен вопросам кибербезопасности, описанию воздействия киберсреды на молодёжь и взрослое население. Он содержит краткий анализ, описание алгоритма и примеры механизмов вовлечения молодёжи в деструктивные сообщества в сети «Интернет», описывает первичные методы защиты.

Оглавление

Введение: чем опасно киберпространство?

Всё, что мы видим с экрана, мы воспринимаем как существующее, как действительное, то, что имеет место быть. В самом радикальном случае, всё остальное прочее (чего мы не видели) место быть не имеет. Проще говоря, всё что вижу, существует, а того, чего не видел – нет. И всё было бы ничего, если бы не одно НО, связанное с киберпространством.

А киберпространство сегодня ориентировано на продажи, прежде всего, это касается всех поисковиков, социальных сетей, по сути, вся система через контекстную рекламу завязана на огромную маркетинговую воронку.

В маркетинге нет нравственности, маркетинг учит продавать абсолютно всё, в том числе товары, услуги и **контент** зачастую абсолютно **аморального** характера. Для этого в технической части используются различные инструменты, такие как программы-шпионы – к примеру, те самые cookies, предупреждение о которых вы видите практически на каждом сайте, который посещаете. Однако от того, что вы прочитаете эти предупреждения, вам не станет слаще, легче или приятнее. Скорее всего, вы просто нажмёте «agree», даже не задумываясь. Хотя многие сайты и вообще не считают нужным оповещать, что ведут за вами слежку и сбор данных. И это касается как сайтов относительно миролюбивых, так и сайтов с деструктивным, откровенно разлагающим контентом. К примеру, алгоритмы YouTube ориентированы не столько на продажу товаров, сколько на монетизацию и продажу контента. Чтобы быть в топе, блогерам приходится постоянно выдавать виральный контент, и наиболее просматриваемым является контент развлекательного, шокирующего, по сути, деструктивного содержания. И это относится не только к YouTube, но и всей корпорации Google, а также Microsoft и другим корпорациям.

Роскомнадзор не может и технически не успевает отслеживать весь деструктивный контент, который наводняет белый интернет, и тем более даже не берётся чистить Darknet. Средства слежки и сбора данных, инструменты маркетинговых воронок постоянно совершенствуются, без труда находят дырки и лазейки в ваше персональное сознание. К сожалению, ни в правовом поле нашего государства, ни в международном праве этот дикий интернет-маркетинг никак не регулируется. И крайне сложно, почти невозможно юридически предъявить поставщикам деструктивного контента – владельцам сайтов

с разрушающим психику и разлагающим нравственность человека контентом – хоть сколь-нибудь серьёзные претензии. Конечно, Роскомнадзор может запретить доступ к сайту, но все знают, как возможно легко технически обойти этот запрет.

Отдельный момент – возрастные ограничения, которые выставляются различными сервисами, якобы, для того, чтобы оградить детей от просмотра или прочтения материалов для взрослых. Фактически данные возрастные ограничения легко обходятся простым нажатием кнопки «Да, мне есть 18» и выполняют скорее роль манка[1] для подростка. И этот момент также никак не регулируется, и сайтам, которые поставили провокационную возрастную заслонку, также нечего предъявить, поскольку формально всё «по закону».

Получается, единственным способом противостоять агрессивной маркетинговой воронке и деструктивному контенту являемся мы сами, как субъекты своей жизни, которые хотят сохранить свой разум чистым. Либо не являемся, если не хотим. Или просто не имеем знаний о кибербезопасности.

Цель нашей сегодняшней встречи и всех последующих, методических материалов и обучающих фильмов, которые создаёт Центр СИ, вооружить себя этими знаниями, разобраться с деструктивными явлениями киберсреды и обучиться медиаграмотности.

Это как с зубоврачебной поликлиникой. Мы можем бесконечно обращаться в поликлинику за помощью к зубным врачам, как делаем это, когда пишем в Роскомнадзор. Но кариес и пародонтоз не перестанут появляться сами собой, пока мы не приобретём полезную привычку регулярно чистить зубы. Так и мы начнём хотя бы с того, что будем регулярно чистить cookies и далее научимся более сложным вещам.

Что такое DNS-кэш? И зачем его чистить?

Чтобы понять, что такое **DNS-кэш**, для начала введём ряд понятий, таких как: д**оменное имя, IP-адрес**, и собственно **DNS** (от англ. Domain Name System «система доменных имён»). Кроме того, нам нужно понимать, как работает интернет.

Интернет – это, грубо говоря, сеть, в которой все машины (включая ваш

1 Манóк — приспособление или инструмент, имитирующий своим звучанием голоса зверей или птиц. Служит для их приманивания, например, на охоте.

персональный компьютер, мобильный телефон, принтер и роутер), сервера (на которых размещены ваши любимые сервисы и сайты), словом всё оборудование во всём мире соединено между собой. И соединяются эти машины через множество локальных и крупных центральных распределительных серверов (узловые точки интернета), которые посылают и отправляют пакеты данных.

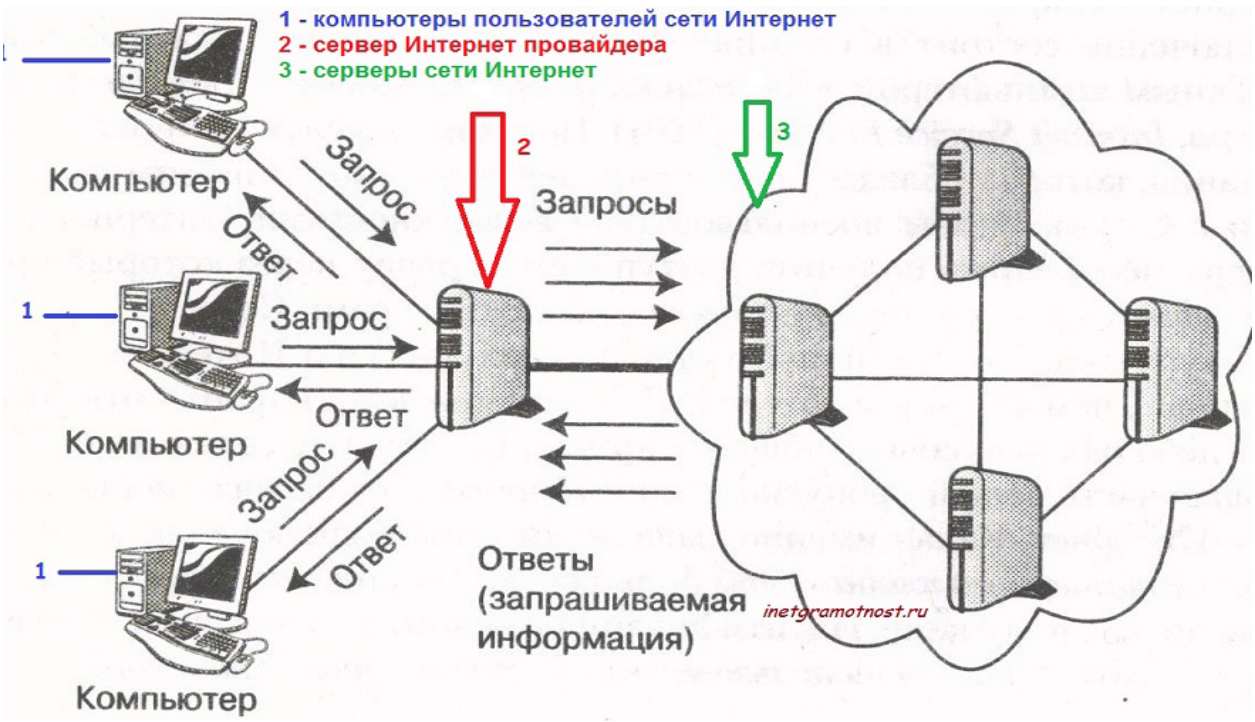

Рисунок 1 Упрощённая схема работы Интернета

Ключевое, что нам нужно сейчас запомнить, что Интернет – это машины (компьютеры, серверы и прочее оборудование), которые соединены и общаются между собой пакетами данных. И машины не общаются между собой на английском, русском или на каком-либо другом человеческом языке. Машины **понимают только язык цифр**.

К примеру, Вы – человек, который хочет попасть на сайт center-si.ru. Вы набираете это **доменное имя** в адресной строке браузера или вводите запрос в поисковик.

Для вашей машины (компьютера или мобильного телефона) эти латинские символы непонятны, ей нужен понятный числовой **IP-адрес**. По аналогии можно привести пример с телефоном и телефонными номерами. Вот Вы, хотите позвонить своему новому знакомому, которого зовут Петрович. Но Вашему мобильному устройству имя Петрович ни о чём не говорит. И сколько бы Вы не кричали в трубку имя «Петрович», ничего не произойдёт. Чтобы связать Вас

с Петровичем Вашему мобильному устройству нужны цифры – телефонный номер этого самого Петровича.

Отсюда следующая аналогия. Допустим, что Вы впервые будете звонить Петровичу, и что номера Петровича у Вас нет, а позвонить надо. Чтобы узнать номер Петровича и записать этот номер в базу контактов (абонентскую книгу) своего телефона, Вы делаете запрос – спрашиваете этот самый номер у друзей или знакомых.

Также действует ваш компьютер, чтобы узнать **IP-адрес** («телефонный номер») конкретного сайта («абонента»). Только свой запрос он посылает **DNS-серверу**, который находит соответствующий IP-адрес и отправляет его обратно Вашему компьютеру, чтобы тот смог загрузить искомую веб-страницу.

Сервера DNS (которых, кстати говоря, очень много) хранят в себе соответствие IP буквенному адресу. В базе данных серверов DNS обязательно прописаны все **IP-адреса к доменным именам** всех сайтов (это такие хранилища-справочники абонентских номеров всех сайтов в мире).

После того, как Вы хотя бы один раз зашли на любой конкретный сайт, IP-адрес этого сайта автоматически заносится операционной системой Вашего компьютера в своеобразную телефонную (абонентскую) книгу, формируя Вашу базу «контактов». Такая «абонентская книга» на Вашем персональном компьютере называется **DNS-кэш**. И получается, что в следующий раз Вы «дозвонитесь» до нужного сайта быстрее, поскольку его конкретный IP-шник уже прописан в «абонентской книге» DNS-кэша, и Вашей машине не нужно будет делать снова запрос на центральный распределительный сервер.

Приведём также третью аналогию. Допустим, Вы ведёте кружок по видеомастерству для школьников «Дело за кадрами!» и решили создать свой собственный интернет-проект и свой собственный сайт. Вы задали своему сайту (по сути, своему детищу) уникальное доменное имя Delozakadrami.ru. Вы выбрали для него «квартиру» – **хостинг**, т.е. место на сервере у поставщика услуг хостинга, где физически будут размещены файлы сайта.

С Вашим проектом, с Вашим детищем всё происходит также, как и с рождением ребёнка. Вы также даёте ему имя, а затем начинается долгий процесс регистрации нового гражданина страны – оформление свидетельства о рождении, внесение соответствующих записей в паспорта родителей и так далее. Только в нашем случае в Интернете прописывается имя нового «гражданина»

интернет-пространства – Вашего сайта на тех самых центральных узловых распределительных серверах – DNS-серверах.

Кроме того, закон также требует прописать ребёнка по конкретному адресу. Также и в глобальном каталоге системы доменных имён, к конкретному имени Вашего сайта присваивается конкретный физический IP-адрес («адрес прописки»). Это занимает некоторое время – от часа до суток.

Таким образом, IP-адрес указывает на физическую прописку Вашего сайта, т.е. на размещение файлов сайта на вполне определённом сервере Вашего хостинг-провайдера.

По аналогии, к примеру, Вы физически живёте по определённому адресу в конкретной квартире у конкретного арендодателя. Вы – это сайт, Ваш адрес – это IP-адрес сайта, квартира в многоквартирном доме – это место, выделенное для Вашего сайта на сервере, арендодатель – это хостинг-провайдер. Если Вы вдруг физически решите переехать на новое место жительства, то Ваше ФИО от этого никак не поменяется (также, как и не изменится доменное имя сайта), но изменится адрес места жительства.

То же самое и здесь – если Вы решите перенести свой сайт на сервер другого хостинг-провайдера (арендодателя), изменится IP-адрес сайта, но доменное имя сайта Delozakadrami.ru останется прежним. Однако, чтобы все центральные распределительные узловые сервера снова прописали уже новый IP-адрес Вашего сайта в свои каталоги, снова необходимо время от часа до суток для перерегистрации сайта по новому месту жительства.

Кстати именно переездом запрашиваемого сайта на другой сервер объясняется ошибка 404. У сайта изменился IP-адрес, а в DNS-кэше остался старый, уже недействительный адрес сайта. Для этого, кстати, необходимо удалить «закэшированный» IP из DNS-кэша.

Мы с Вами подробно разобрали, что такое доменное имя, IP-адрес, DNS-кэш. Но, собственно, что же такое **Domain Name System** или «система доменных имён»? И для чего она нужна?

Дело в том, что, когда в каталоги центральных распределительных узловых серверов, DNS-серверов, прописывается путь (IP-адрес) каждого конкретного сайта, это позволяет отсылать и принимать запросы (пакеты данных) между машинами (компьютерами и серверами) глобальной сети интернет за считанные миллисекунды. А иначе, без этого глобального каталога доменных

имён, каждый запрос пользователя обрабатывался от часа до суток и более. Грубо говоря, один раз проложил железную дорогу, и затем почта по ней быстро перемещается от одного IP-адреса к другому.

Теперь мы подобрались к главному вопросу: **Зачем же чистить DNS-кэш?**

Как мы выяснили **DNS-кэш** – это телефонная (абонентская) книга на Вашем компьютере, куда автоматически записываются IP-адреса всех сайтов, на которые Вы когда-либо заходили. Делается это (и придумано изначально) для того, чтобы сделать Вашу работу в интернете более комфортной и быстрой.

Повторим, в DNS-кэш записываются IP-адреса **всех сайтов**, на которые Вы **когда-либо** заходили осознанно, случайно, все рекламные ссылки, на которые Вы когда-либо кликали. Нет никакой фильтрации и разделения сайтов на плохие, хорошие, деструктивные или полезные.

Представьте, что в базу контактов вашего телефона без Вашего ведома постоянно, автоматически вбивались бы номера всех людей подряд, с которыми Вы прямо или косвенно соприкасались бы. Помимо нужных телефонов родных, коллег, учительницы вашего сына и сантехника дяди Коли, вбивались бы номера продавщицы из магазина, алкоголика, которого Вы увидели на автобусной остановке, кондуктора из автобуса, городской шпаны и того страшного маньяка, о котором Вы намедни видели документальную телепередачу. Более того, каждый раз, когда Вы бы брали телефон в руки, он стал бы последовательно прозванивать по номерам телефонов всех этих контактов. Хотели бы Вы, чтобы он позвонил тому маньяку и попутно ещё слил бы адрес вашего местонахождения (IP-адрес)?

Вот примерно то же самое происходит, когда Вы заходите в интернет и запускаете браузер. Браузеры автоматически подгружают из DNS-кэша (абонентской книги) те сайты, странички и вкладки, которые Вы просматривали в прошлую сессию вчера вечером.

И если Вы вчера мимоходом глянули справку на каком-нибудь специфическом сайте про какого-то известного маньяка во время сёрфинга в интернете, адресок этого сайта уже подгрузился в DNS-кэш. И теперь, когда Вы снова зашли в интернет, контекстная реклама в браузере, имеющем доступ к DNS-кэшу,

в качестве рекомендации любезно даст Вам ссылку на ролик TED в YouTube, где субъект с сомнительными наклонностями рассказывает аудитории о том, как трудно ему, «бедному педофилу», на свете живётся или предложит Вам интернет-магазинчик, коллекция товаров которого позволит удовлетворить самую извращённую фантазию.

При этом, хорошо, если Вы – взрослый человек с критическим мышлением и с устойчивой психикой. А если речь идёт о Вашем ребёнке? Или о Ваших учениках и воспитанниках? Куда заведёт их безнравственная автоматическая контекстно-маркетинговая воронка? Или же целенаправленная политика корпораций, ведущих через свои браузеры (к примеру «Хром» от Google) сбор данных Cookies и DNS-кэша?

Материал РИА «Катюша». Ведите ваших деточек: Google и YouTube попались на сборе информации о детях без согласия родителей

Уже откровенно посылающая Роскомнадзор и отказывающаяся не только переводить серверы в Россию, но даже блокировать запрещенное видео, американская корпорация Google угодила дома в новый скандал. Генеральный прокурор Нью-Йорка вместе с Федеральной торговой комиссией оштрафовали на $170 млн видеохостинг YouTube за сбор персональной информации о детях без согласия их родителей.

Рисунок 2. Автор картинки - РИА «Катюша»

«После длившейся более двух лет проверки по запросам возмущенных содержанием «детского контента» YouTube родителей, дело сдвинулось с мертвой точки и чуть не на уровне первых лиц США американскую корпорацию Google вынудили признать – да, она целенаправленно собирает информацию о посещающих сайт детях без информирования их родителей. Так, собиралась информация об интересах и пристрастиях детей, после чего им «предлагалась» соответствующая реклама, согласованная с политикой компании.

В переводе на человеческий, если ваша дочь решила учиться печь торты и смотрела ролики с рецептами от известных поваров (что более, чем похвально), то YouTube ей с одной стороны, мог предложить кучу рекламы на тему покупки ингредиентов и разных форм для выпечки кексов, а с другой, например, ролики, где эти известные повара будут готовить вместе с известной звездой-трансгендером или переживать за протестующих в Гонконге, что уже не так радостно. Собственно, именно таким образом у нас и раскрутилось «развлекательное» и крайне познавательное, особенно для родителей, шоу «Сливки Кидс» на канале Youtube «REAL TALK», где опубликованы видеоролики, в которых дети ведут откровенные разговоры с бывшей порноактрисой Ангелиной Дорошенковой, травести-артистом Дмитрией Рублевским (Мисс Рублевская) и педерастом[2] Максимом Панкратовым. Притом шоу – мегапопулярное, имеющее по полтора-два миллиона просмотров. К этому стоит только добавить то, что на сегодня данный канал, который открыто и активно ведет пропаганду педерастии и извращений, не только не закрыт, но и выпустил новый «хит», в котором очередной представитель ЛГБТ рассказывает, что сегодня в России чуть ли не рай для педерастов и их все активно поддерживают.

Впрочем, если штраф и признание того, что Google и YouTube собирают информацию о детях и ведут среди них «воспитательную работу» – стали для кого-то новостью, то отказ американцев чего-то там закрывать по требованию российских властей уже больше похож на анекдот. Просто потому что Google открыто игнорирует все требования, показывая, что какая-то там власть им никто и звать их никак…»

Вот и простой ответ на вопрос, почему нужно чистить DNS-кэш.

2 Для тех, кто борется за толерантность, обращаем внимание, что данная цитата взята из оригинального текста.

Инструкция: как почистить DNS-кэш?

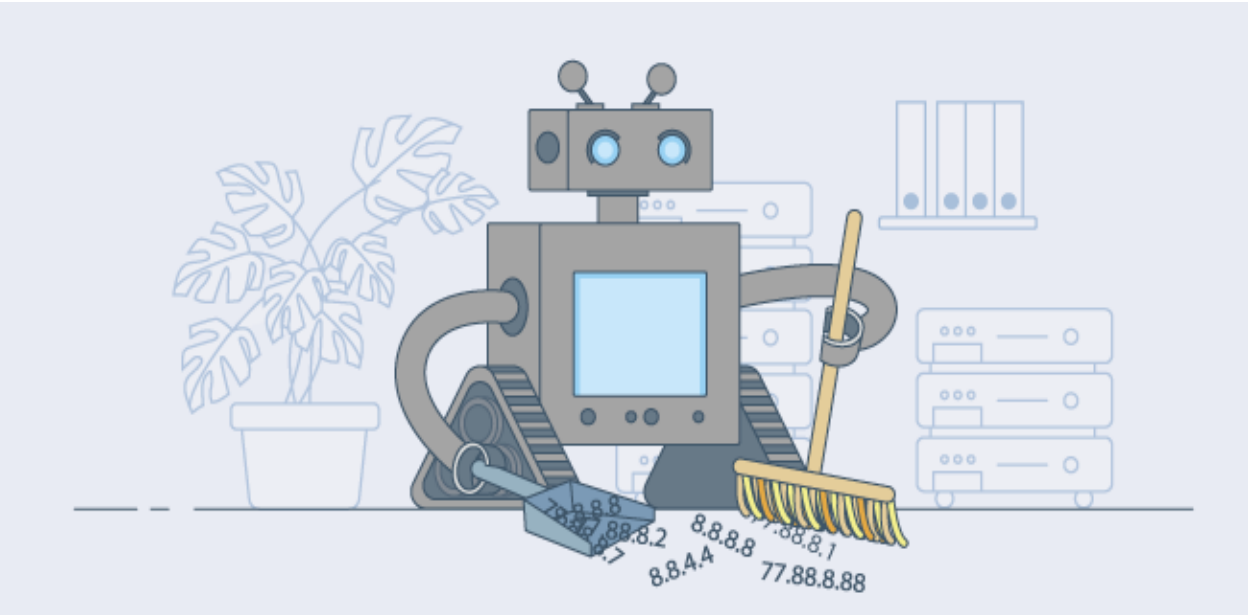

Рисунок 3. Изображение с сайта ispsystem.ru

Как очистить DNS-кэш в операционной системе?

Очистить DNS-кэш в любой операционной системе просто. Для этого нужно ввести всего одну команду через консоль.

Windows 10

1. Откройте меню **Пуск**, в строке поиска введите **cmd**. Поиск выдаст пункт **«Командная строка»** (cmd.exe). Кликните на него правой кнопкой мыши и выберите пункт **«Запуск от имени администратора»**.

2. В открывшемся окне командной строки введите команду **ipconfig/flushdns** и жмите **Enter**. Сделано!

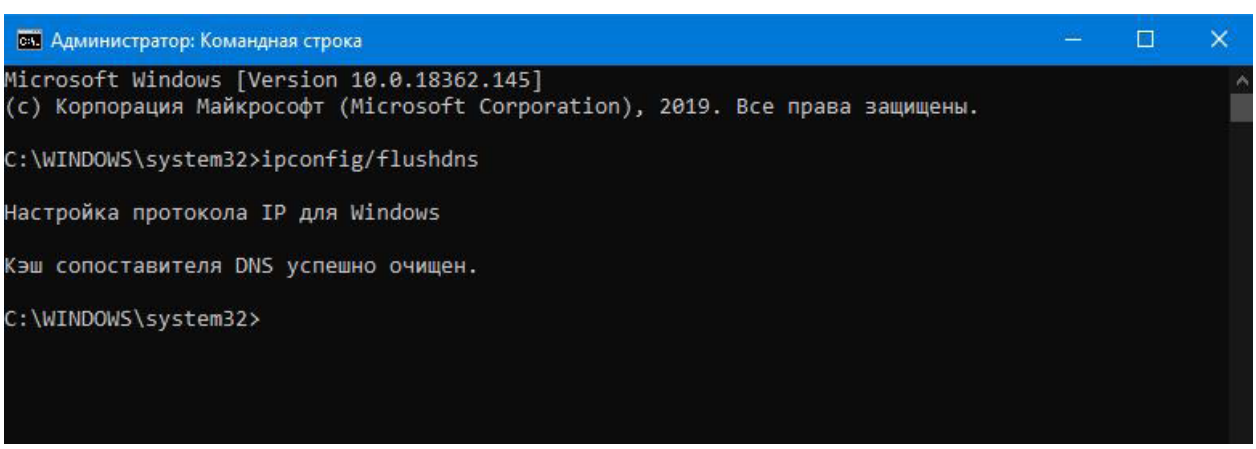

Рисунок 4. Очистка DNS-кэша через командную строку Windows

Ubuntu

1. Одновременно зажмите сочетание клавиш c**trl +alt +T.** Откроется **Терминал.** Также Вы можете найти его в списке приложений.

2. В терминале введите команду **sudo systemd-resolve --flush-caches**, а после укажите пароль администратора. Сделано!

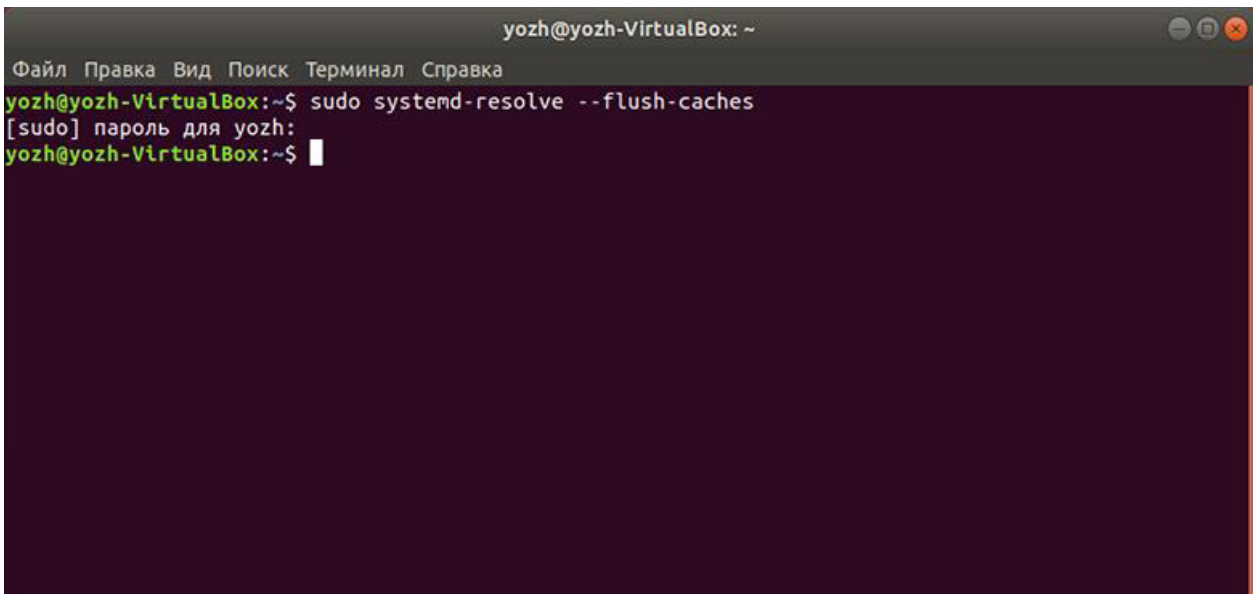

Рисунок 5. Очистка DNS-кэша через Терминал Ubuntu

MacOS 10.14 Mojave

1. Кликните на иконку поиска в правом верхнем углу, далее найдите в поиске **Терминал**.

2. В открывшемся окне введите команду **sudo killall -HUP mDNSResponder; sleep 2**; а затем введите пароль администратора. Сделано!

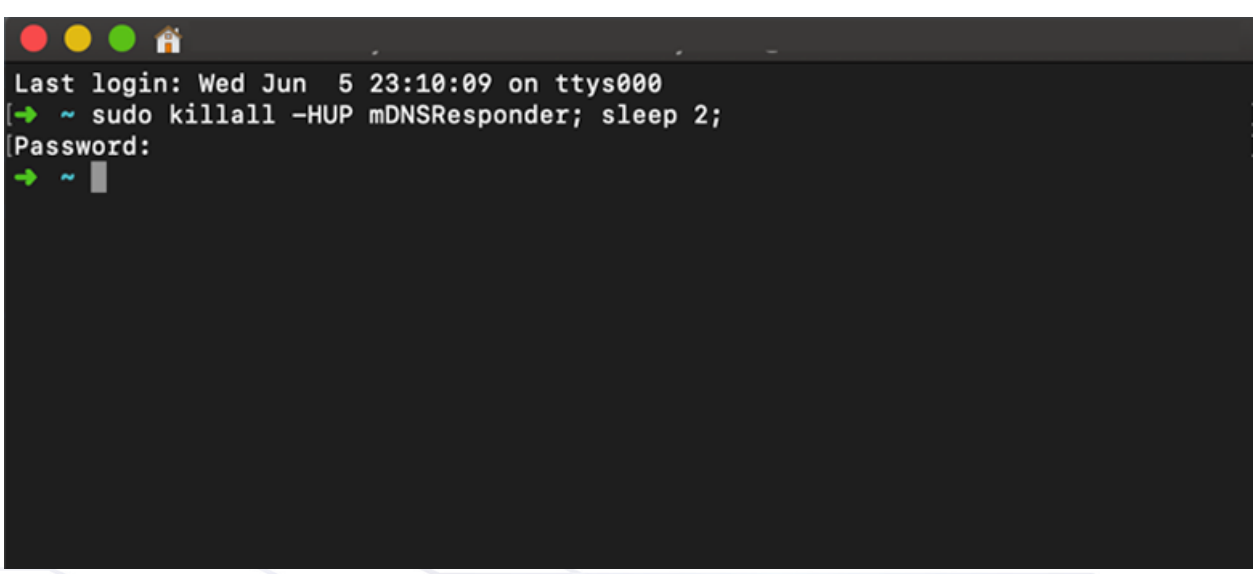

Рисунок 6. Очистить DNS-кэш через Терминал macOS

Как чистить DNS-кэш в браузере?

У всех современных браузеров также есть собственный DNS-клиент, который кэширует IP-адреса посещённых сайтов. После того, как Вы очистите кэш в Вашей системе, необходимо дополнительно почистить DNS-кэш и в браузере.

Google Chrome, Opera и Яндекс.Браузер

Данный метод подходит для браузеров, основанных на Chromium.

1. В строке браузера введите адрес **chrome://net-internals/#dns.**
2. В открывшемся окне кликните на команду **Clear host cache**.
3. В том же окне выберете пункт **Sockets** и далее нажмите F**lush socket pools**. Сделано!

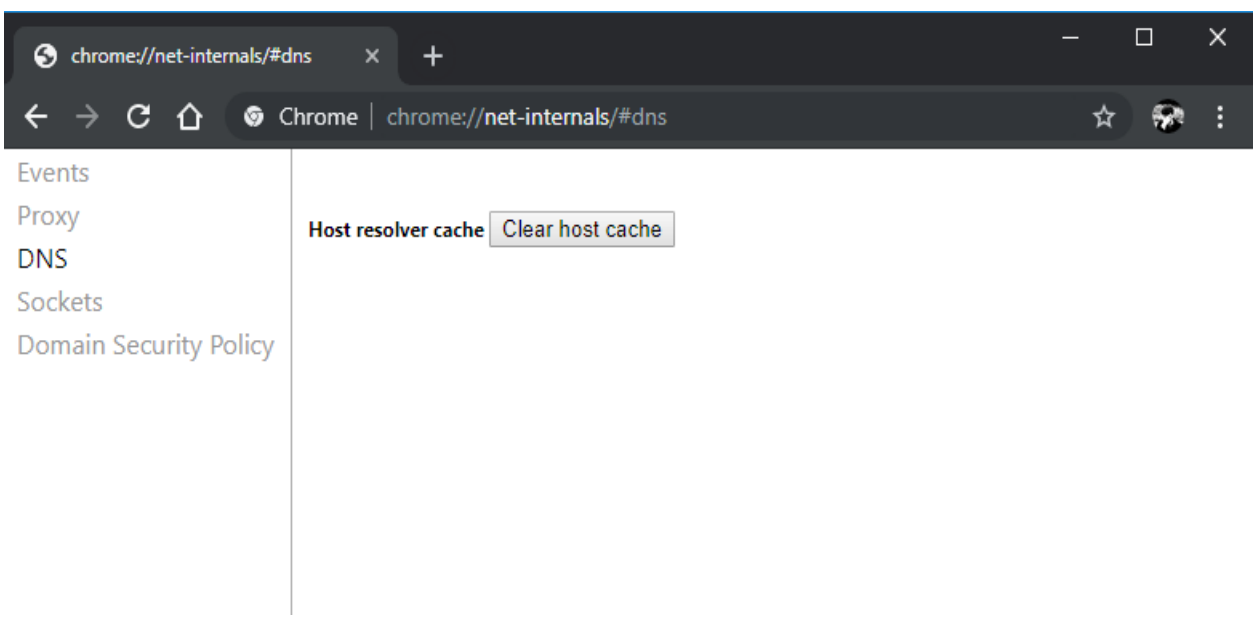

Рисунок 7. Очистка DNS-кэша в браузере Google Chrome

Mozilla Firefox

1. В меню браузера выберите пункт **Настройки**.
2. В разделе **Приватность и защита** найдите пункт **Куки и данные сайтов.**
3. Далее нажмите кнопку **Удалить данные**. В открывшемся окне снимите галочку с пункта Куки и данные сайтов и нажмите кнопку **Удалить**.

Сделано!

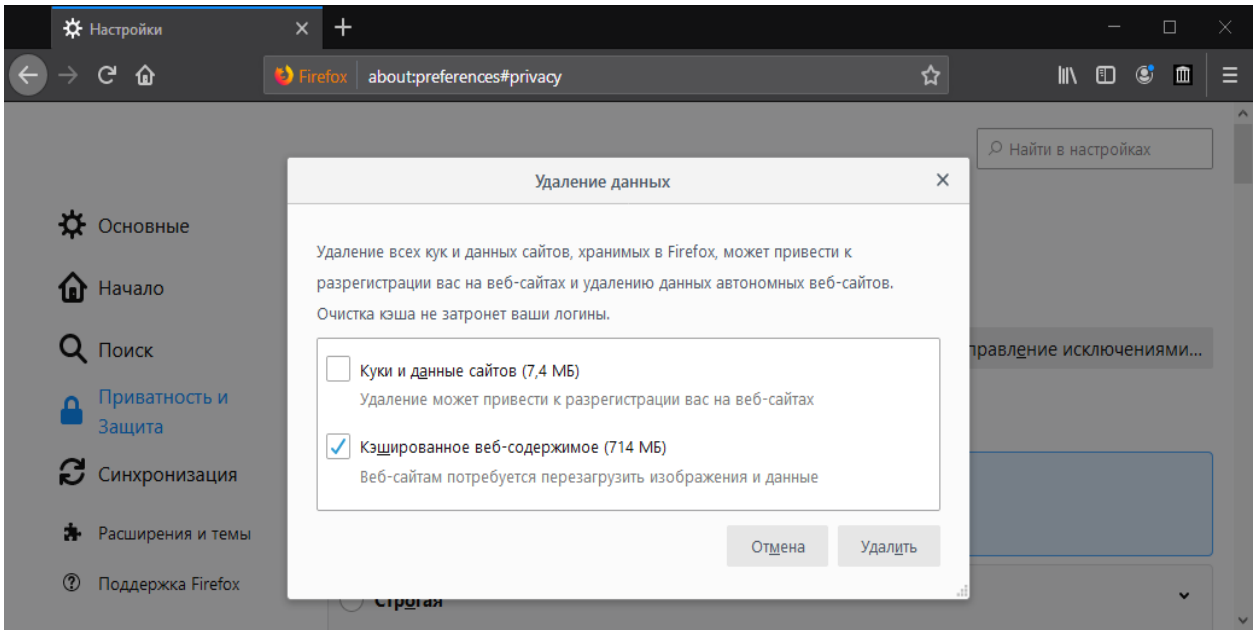

Рисунок 8.Очистка DNS-кэша в браузере Firefox

Cookies

Cookies – это маленькие файлы с данными, куда записывается информация о наших действиях на определённом сайте.

Файлы cookie генерируются в процессе обмена данными между браузером и этим сайтом. Т.е. у каждого сайта только свои cookies, которые сохраняются у нас на компьютерах и на других наших устройствах и запускаются, когда мы вновь открываем браузер.

Изначально файлы cookie (к слову, этой технологии уже 25 лет) придуманы для того, чтобы облегчить нам жизнь и ускорить работу в интернете. Сегодня же cookies – это не только серьезная угроза для конфиденциальности, но и реальный инструмент влияния на нашу психику и психологию извне.

Файлы cookie – это основной источник сведений о пользователе, необходимых маркетологам для создания контекстной рекламы.

Что же знают о нас эти крохи?

• местоположение и IP-адрес пользователя;

• версию ОС и браузера;

• предпочтения и настройки пользователя, такие как, язык, валюта или размер шрифта;

• дату и время посещения сайта;

• текст, который вы вводили на сайте;

• товары, которые вы добавили в корзину или просматривали;

• клики и переходы.

Как много данных о Вас знают и обезличены ли они?

Казалось бы: если у каждого сайта только свои cookies, и подгружать с нашего компьютера он может только именно эти cookies (и не имеет доступа к cookies других сайтов), то выходит, что владельцы сайта получают лишь **ограниченный доступ к обезличенной информации** и поведении пользователя только на их конкретном сайте. Ну и пусть, что плохого-то? Сплошной комфорт! Зачем мне дважды выбирать и добавлять в корзину одни и те же товары или логиниться?

Да это так. Но разберёмся подробнее. Когда мы говорим о cookies с сайта какого-нибудь частного предпринимателя, то можно не опасаться тотальной слежки или слива наших персональных данных. Но того же самого мы не можем сказать о крупных сетевых организациях, корпорациях и IT-гигантах – владельцах множества сервисов, данные с которых сливаются в общую базу. Google, Яндекс, MailGroup, Сбербанк – самые яркие и известные примеры. Google-почта, Google-поисковик, Google-документы, YouTube. Или Яндекс-поисковик, Яндекс-почта, Яндекс-диск, Яндекс-такси, Яндекс-еда, Яндекс-расписание и Яндекс.Афиша. И ещё десятки сервисов, которые эти гиганты разрабатывают или покупают. Достаточно ли информации они знают о Вас? Вопрос риторический.

Кстати, каким браузером Вы пользуетесь в данный момент? Google Chrome, Яндекс.Бар? Вот кто точно имеет доступ ко всем сохранённым cookies, ведь сама генерация файлов cookie происходит в процессе обмена данными между браузером и веб-ресурсами.

Разберём миф насчёт **обезличенности данных**. Конечно, в cookies не записывается Ваша фамилия, имя и отчество. Когда Вы впервые посещаете какой-нибудь сайт, веб-сервер присваивает Вам свой уникальный идентификационный номер, сохраняет его в cookies, и при всех ваших последующих запросах этот номер из cookies будет отправляться серверу.

А теперь вспомним, что могут запоминать cookies:

• местоположение и IP-адрес пользователя;

• версию ОС и браузера;

• предпочтения и настройки пользователя, такие как, язык, валюта или размер шрифта

и так далее.

А теперь узнаем, как по этим данным идентифицировать конкретного пользователя. Замечательную аналогию на этот счёт приводит журнал xakep.ru:

«Возьмем для примера базу данных, где хранится почтовый индекс, пол, возраст и модель машины. Почтовый индекс ограничивает выборку в среднем до 20 тысяч человек — и это цифра для очень плотно населенного города: в Москве на одно почтовое отделение приходится 10 тысяч человек, а в среднем по России — 3,5 тысячи.

Пол ограничит выборку вдвое. Возраст — уже до нескольких сотен, если не десятков. А модель машины — всего до пары человек, а зачастую и до одного. Более редкая машина или мелкий населенный пункт могут сделать половину параметров ненужными.

Вместо почтового индекса и модели машины можно использовать версию браузера, операционную систему, разрешение экрана и прочие параметры, которые мы оставляем каждому посещенному сайту, а рекламные сети усердно все это собирают и с легкостью отслеживают путь, привычки и предпочтения отдельных пользователей».

Итак, мы поняли – о нас знают много, и – точно именно о нас. Для чего нужна эта информация? Чтобы управлять.

Ну, например, зная поведенческие факторы, привычки и предпочтения пользователя, можно заставить его совершить покупку, даже если изначально он отказался от этой мысли. Это называется ремаркетинг. Цель ремаркетинга заключается в том, чтобы снова вернуть на сайт пользователя, который не совершил целевого действия (не стал делать покупку, не перешел к товарам и услугам) и «подтолкнуть» (по сути, заставить) его покупать.

Данные о потенциальном потребителе (о том, какую новость или рекламу он просматривал, где совершал целевые действия, а где нет) сохраняются в cookies и обязательно будут использоваться в дальнейшем. Дальше человека сопровождает контекстная реклама, где присутствуют ранее просмотренные им предложения. Информация из файлов cookie также применяется для формирования индивидуальной рекламной рассылки.

Пока что реклама следует за привычками пользователя и строится на манипуляциях с уже сформированными предпочтениями. Но сегодня уже идёт речь об использовании данных, чтобы изначально формировать нужные рекла-

модателям привычки и предпочтения.

И для этого будут использоваться все данные о пользователе, до которых только возможно дотянуться. В том числе, конечно, и данные cookies.

Мы понимаем, что безопасность и комфорт вещи трудносовместимые. Но если переносить эти категории на реальную жизнь, вопроса распределения приоритетов не должно возникать.

Инструкция по очистке/отключению cookies в Яндекс-браузере и браузере Google Chrome

Яндекс-браузер

Чтобы очистить cookies в Яндекс Браузере:

1. Откройте «Настройки» браузера 

2. В данной вкладке выберите «Очистить историю».

3. Выберите период и пункт «Файлы cookie и другие данные сайтов и модулей» для удаления.

4. Нажмите на кнопку «Очистить».

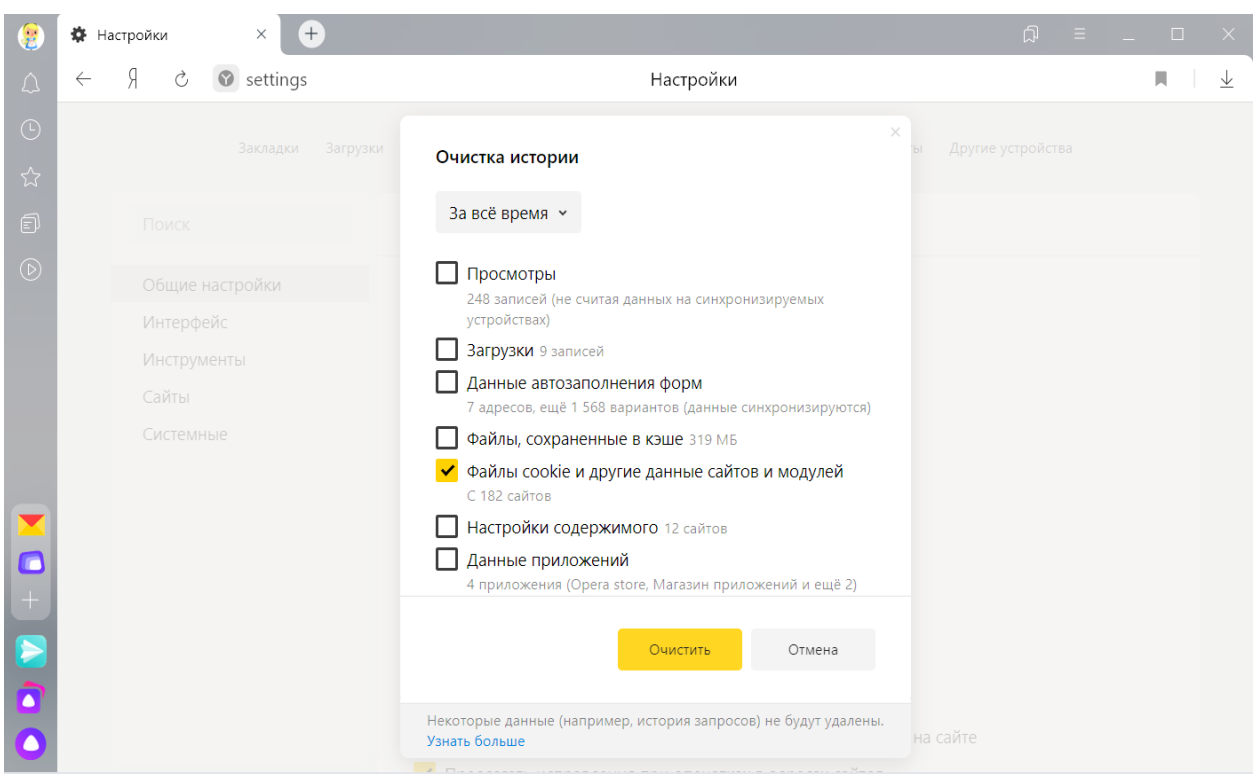

Рисунок 9. Очистка cookies в Яндекс Браузере

Запретить сохранение cookie всем сайтам:

1. В правом верхнем углу нажмите ☰ → Настройки.
2. Откройте раздел «Сайты».
3. Прокрутите страницу вниз и откройте раздел «Расширенные настройки сайтов».
4. В блоке Cookie-файлы включите опцию «Запрещены».

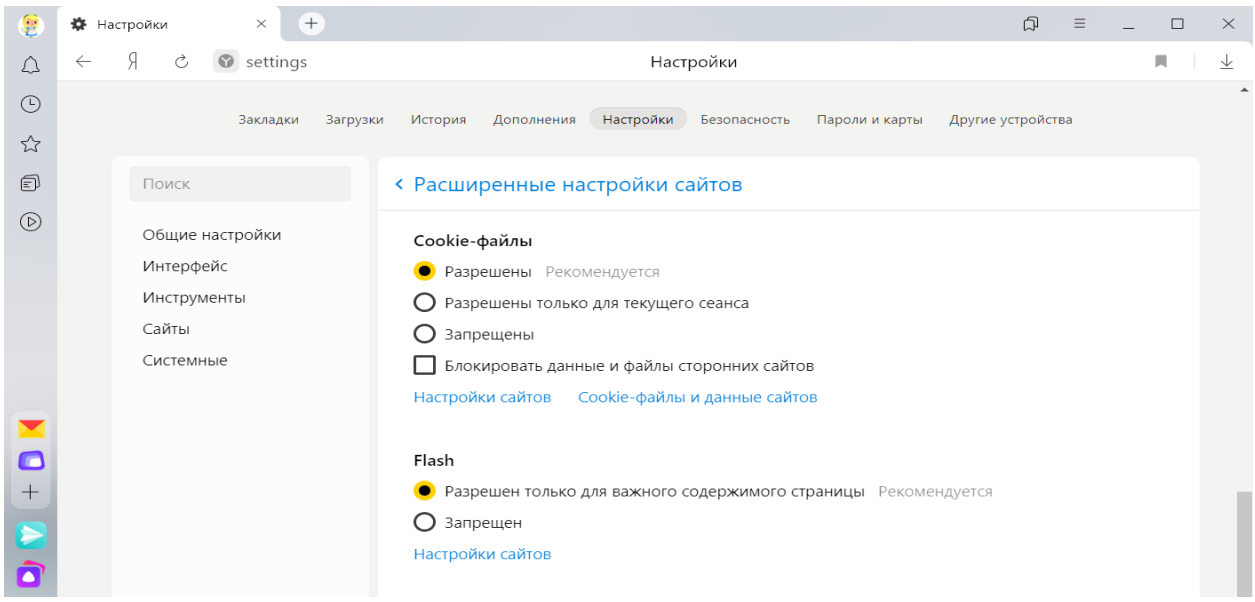

Рисунок 10. Запретить сохранение cookie в Яндекс Браузере

Браузер Google Chrome

Как очистить cookies в Google Chrome:

1. Откройте «Настройки» браузера.

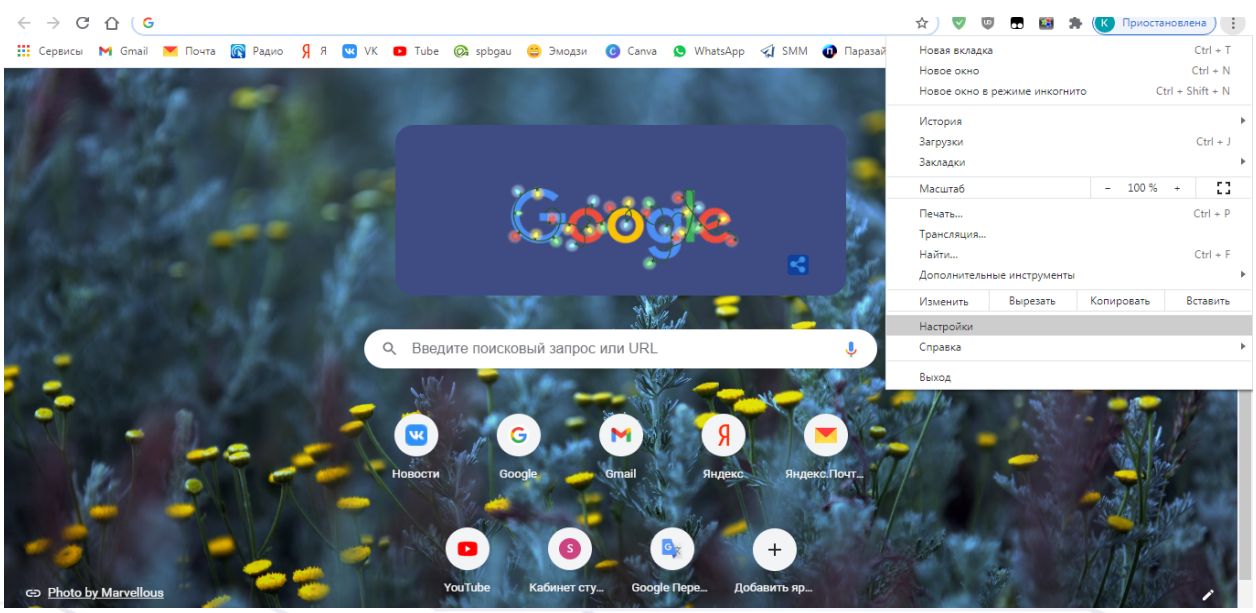

Рисунок 11. Очистка cookies в Google Chrome (Настройки)

2. Нажмите на раздел «Конфиденциальность и безопасность».

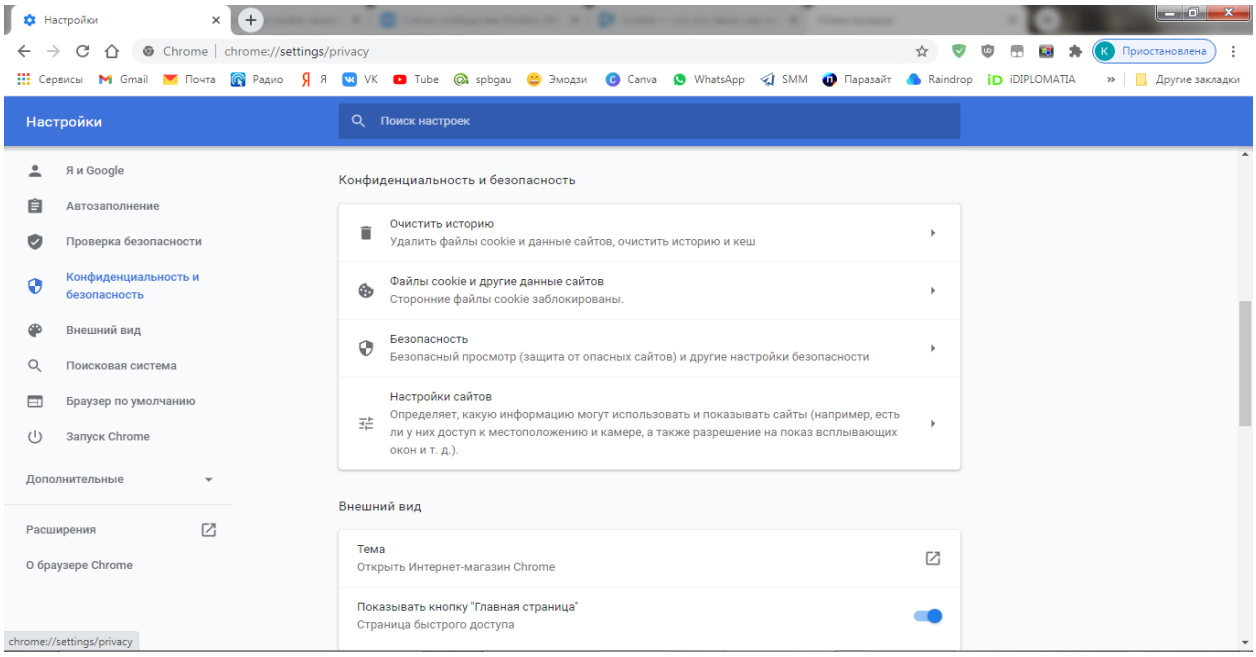

Рисунок 12. Очистка cookies в Google Chrome (раздел «Конфиденциальность и безопасность»)

3. В данном разделе найдите пункт «Очистить историю».

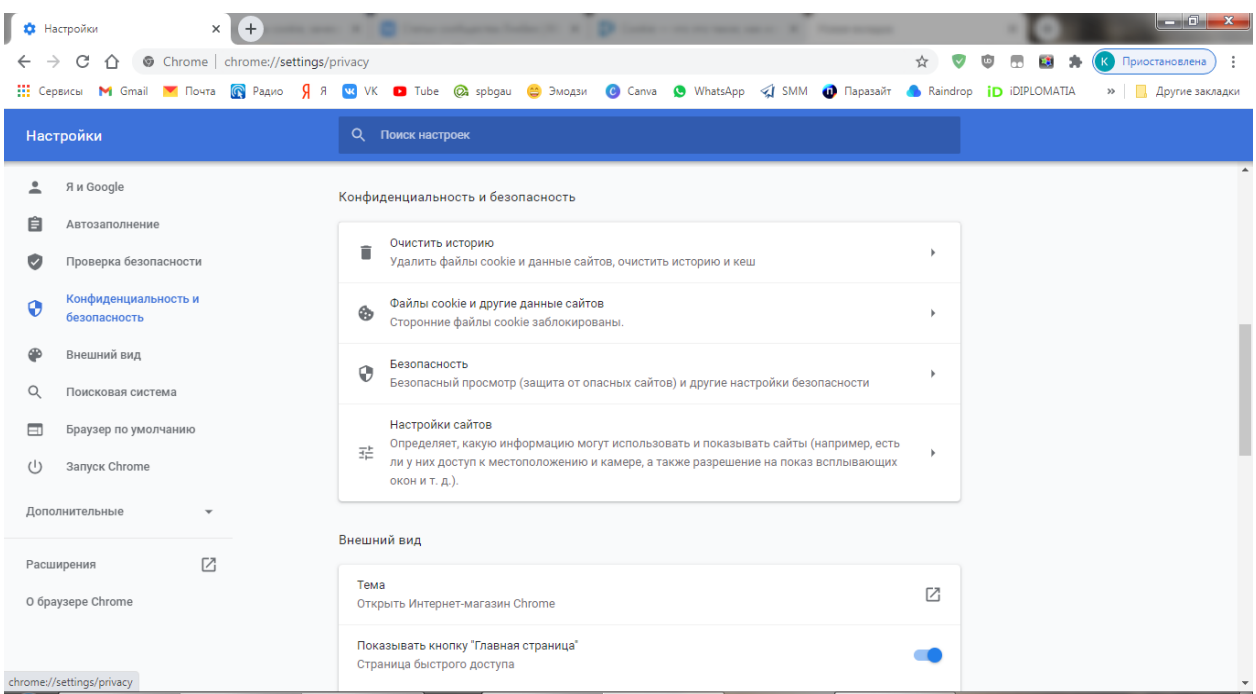

Рисунок 13. Очистка cookies в браузере Google Chrome (пункт «Очистить историю»)

4. Далее выберите пункт «Файлы cookie и другие данные сайтов» для удаления.

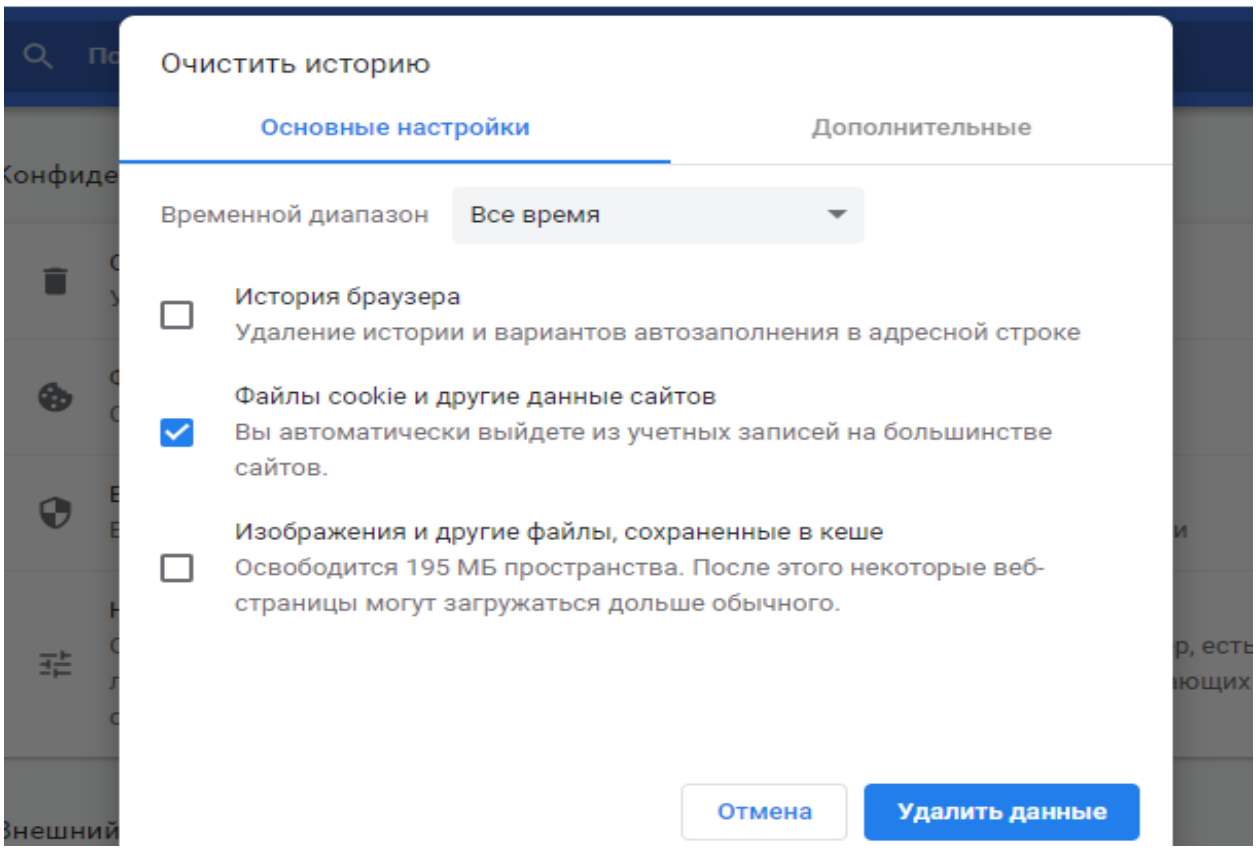

Рисунок 14. Очистка cookies в браузере Google Chrome (пункт «Файлы cookie и другие данные сайтов»)

5. Нажмите на кнопку «Удалить данные».

Отключить cookies в браузере Google Chrome:

1. Откройте «Настройки» браузера.

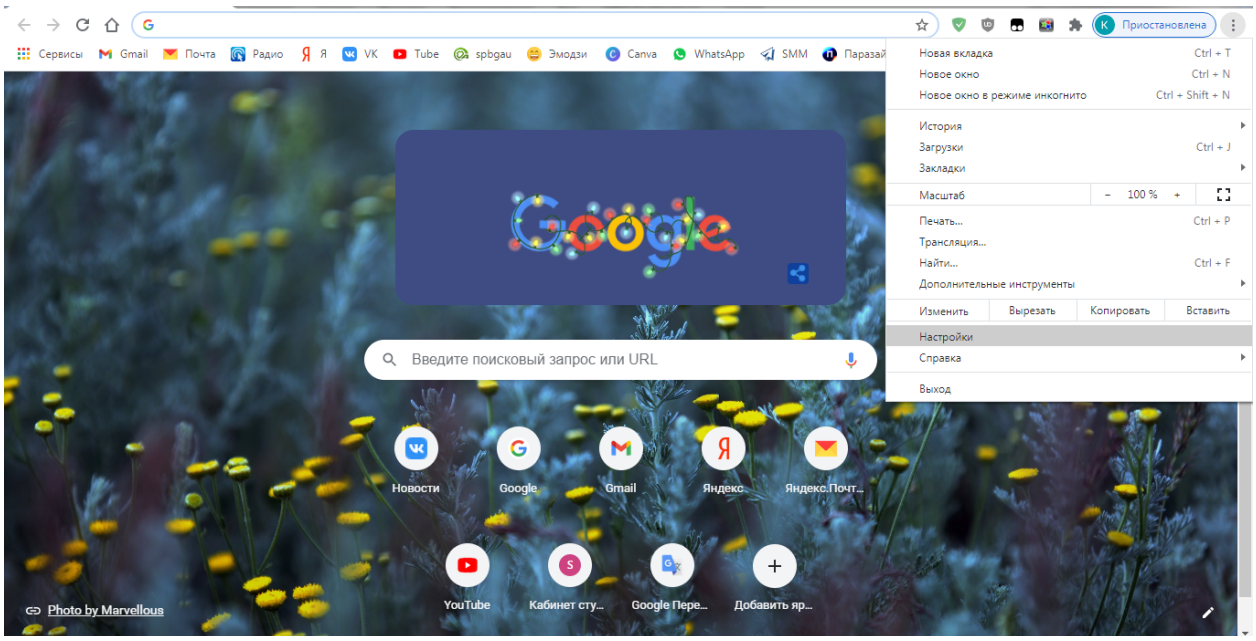

Рисунок 15. Удаление cookies в браузере Google Chrome (Настройки)

2. Нажмите на раздел «Конфиденциальность и безопасность».

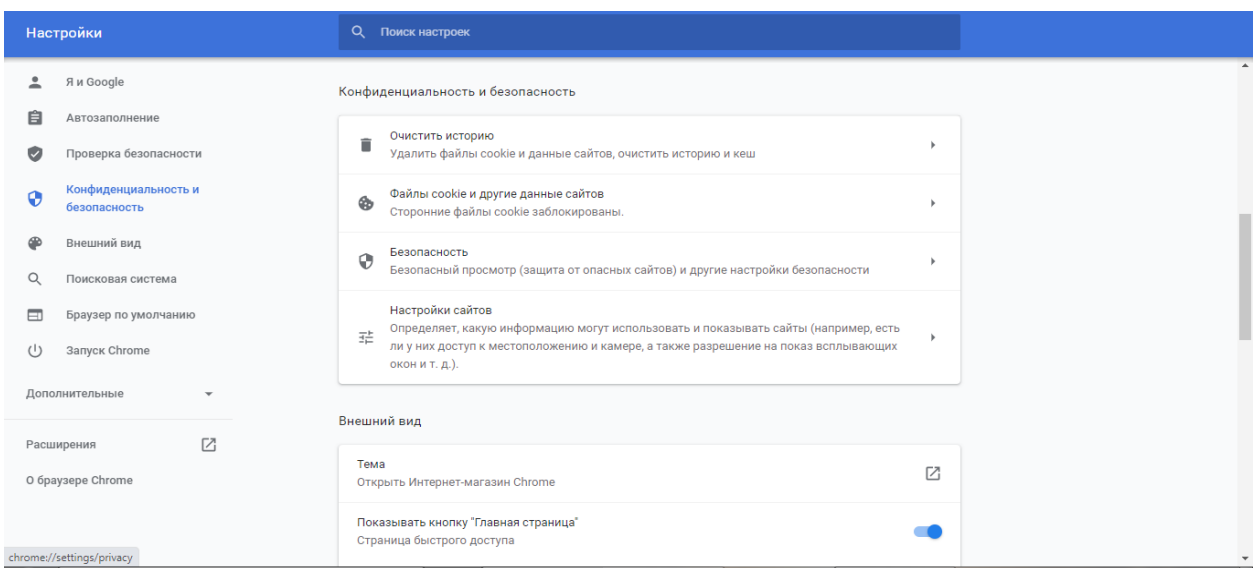

Рисунок 16. Удаление cookies в браузере Google Chrome (раздел «Конфиденциальность и безопасность»)

3. В данном разделе найдите пункт «Настройки сайтов».

4. Затем откройте вкладку «Файлы cookie и данные сайтов».

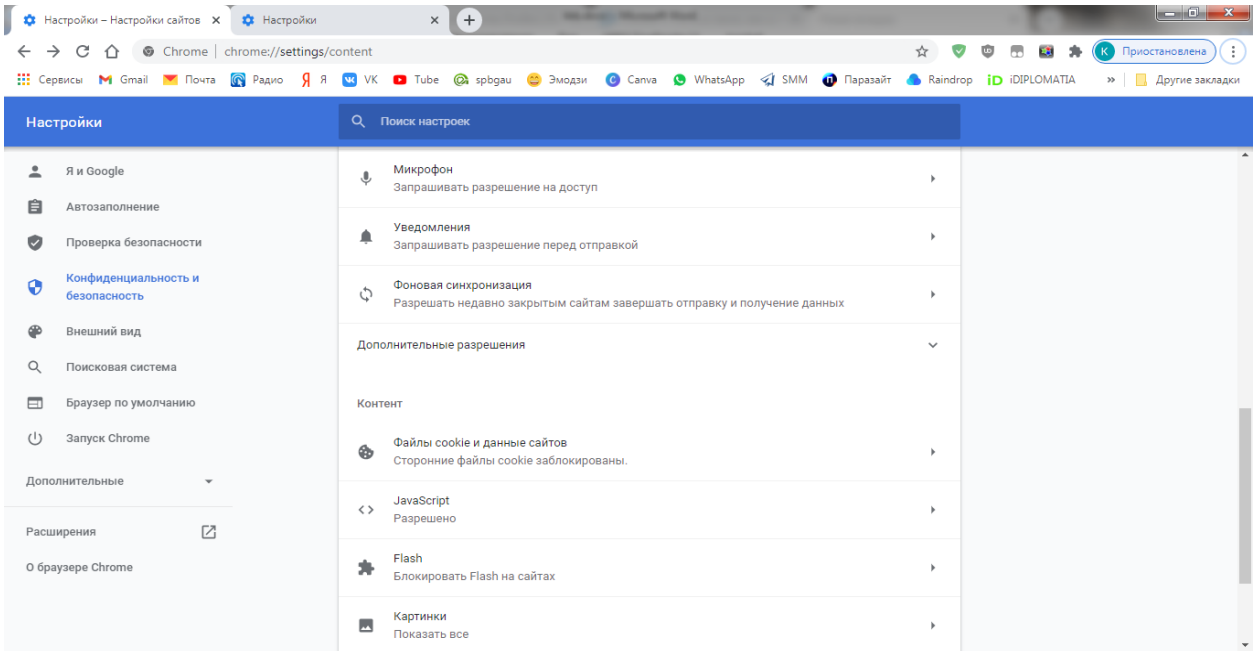

Рисунок 17. Удаление cookies в браузере Google Chrome (раздел «Файлы cookie и данные сайтов»)

5. В открывшемся окне Вы можете блокировать cookie файлы.

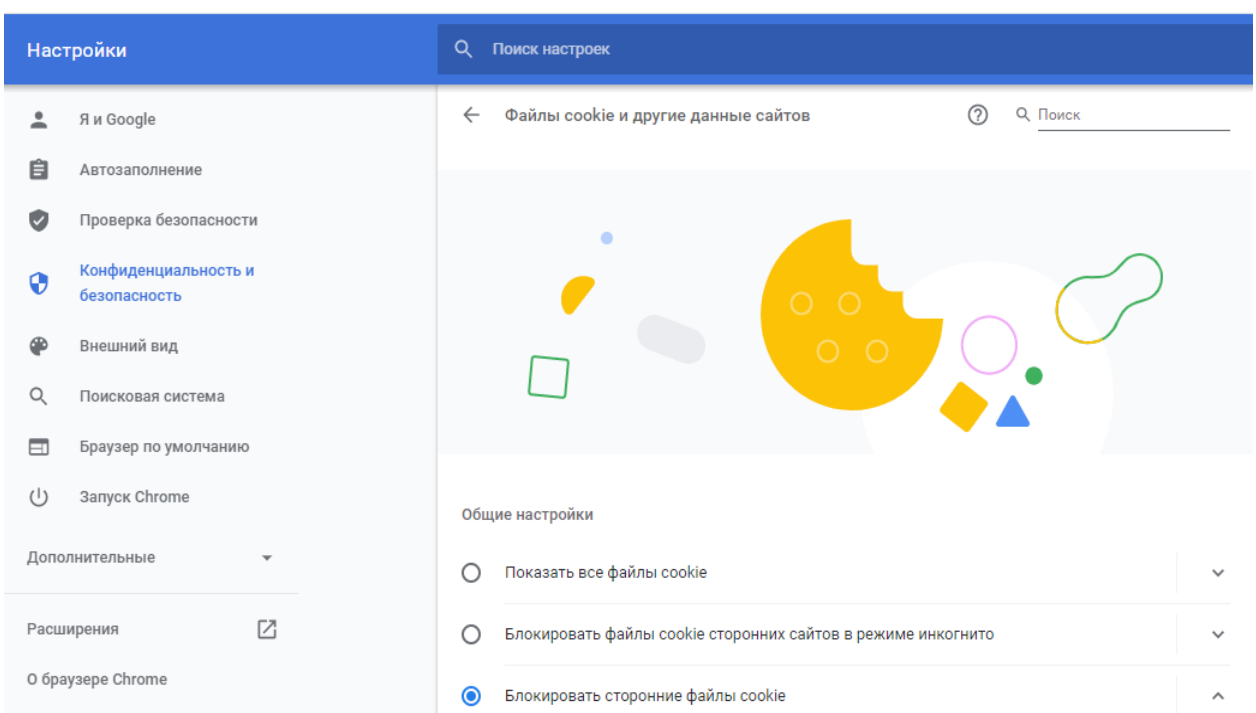

Рисунок 18. Удаление cookies в браузере Google Chrome (блокировать cookie файлы)

Социальный аспект: скрытая угроза

На основании десяти лет исследований в области социальной кибербезопасности мы можем констатировать тот факт, что, к сожалению, большинство людей на бытовом уровне недооценивают социальных угроз интернет-технологий.

Особенно ярко это пренебрежение прослеживается на тематике сбора данных о пользователях различными корпорациями. Вот, например, как стандартно мыслит пользователь: *«Ну да, данные собираются всё время. А что, собственно, такого? Наоборот, одни удобства, в почту заходишь быстрее, да и контекстная реклама предлагает именно тот шампунь с эффектом ламинирования и именно тот боевик с Брюсом Уиллисом, которые я и искал вчера целый вечер. Это очень удобно. Современный человек не может отказаться от интернет-благ, только для того, чтобы сохранить приватность».*

Мы, кстати, и не призываем Вас к отказу от интернета и IT-технологий. Эти технологии, действительно, дают человечеству огромные возможности для образования, коммуникаций и развития. С одной определяющей оговоркой. Интернет даёт эти возможности **при соблюдении техники безопасности**.

И наша цель – сформировать **культуру обращения с интернетом** и прописать самые важные и **основные правила техники безопасности**. Как известно, правила техники безопасности или безопасности жизнедеятельности во все времена, к сожалению, «писались кровью», то есть после того, как страшное событие происходило и приводило к людским потерям. Но если в физическом мире ошибки в технике безопасности приводят к очевидным и всеми видимым последствиям, то в современном информационном мире распознать разнообразные прогрессирующие девиации довольно сложно, пока отклонения в психике конкретного человека не достигнут критической точки. Лишь тогда окружающие начинают замечать эти девиации, но, как правило, к этому времени человек уже проходит точку невозврата.

Повторим, эти девиации возникают и прогрессируют вследствие того, что в обществе просто не выработаны и не приняты правила техники безопасности при обращении с Интернетом. Промедление в этом вопросе, особенно учитывая тот факт, что Интернет – это массовая технология, приведёт к столь же массовым потерям среди всего человечества.

В зависимости от степени поражения психики жертв, Центр СИ ввёл две категории:

1. **Контуженный** — человек, психика и интеллект которого поражены, психо-эмоциальные реакции заторможены, однако есть возможность восстановления психики и выздоровления.

2. **Инвалид** (от лат. invalid «непригодный») информационной войны – человек, который приобрёл значительные психические и интеллектуальные отклонения и непригоден для жизни в полноценном обществе.

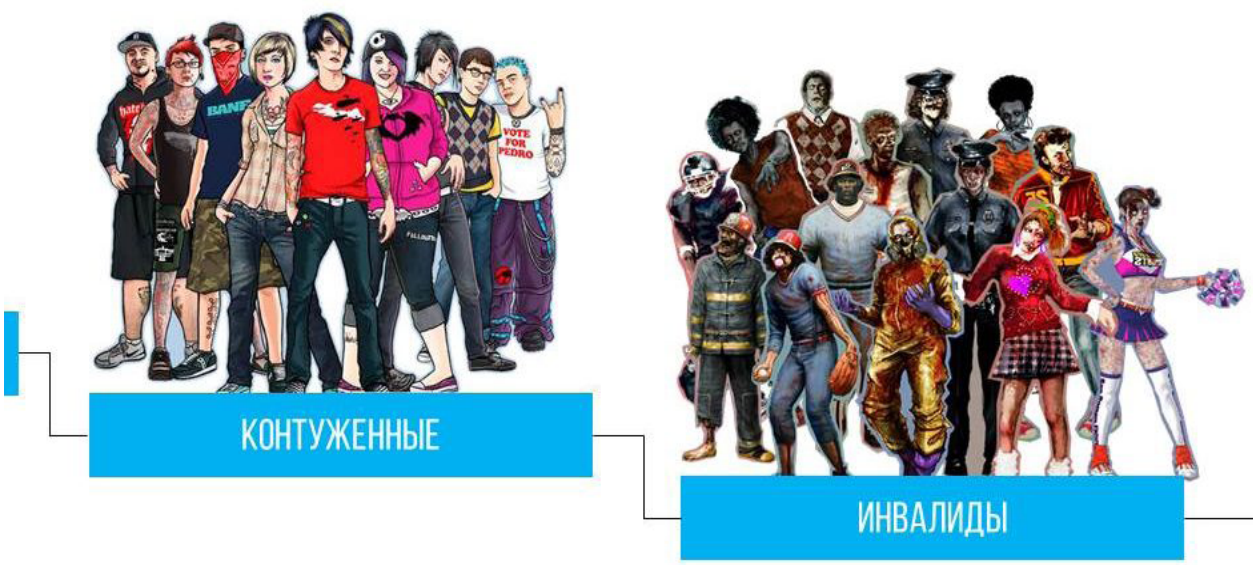

Рисунок 19. Изображение из аналитической работы Центра СИ «Защита идеалов справедливости: новые формы и методы»

Чтобы избежать необратимых потерь и сформировать правила техники безопасности в интернете, необходимо в первую очередь понимать, по каким алгоритмам работают технологии и логику развития/деградации как общества в целом, так и каждого отдельного человека под влиянием этих технологий.

Вернёмся к нашему пользователю с шампунем и боевиками, который не видит никакой опасности в том, что корпорации, компании и сервисы собирают его данные, и, уж конечно, он вряд ли вообще чистит DNS-кэш. К каким последствиям для этого конкретного пользователя приведут алгоритмы, заложенные в интернет-технологии, которыми он так бездумно пользуется?

1. **Информационные пузыри**. Во-первых, со временем, этот пользователь будет окружён только контекстным полем своих запросов. Под его интересы алгоритмы контекстной рекламы, поисковиков, видеохостингов будут

подбирать товары, услуги и, конечно, контент. Постепенно вокруг него будет формироваться информационный пузырь только его прежних интересов, психически пользователь будет погружён «сам в себя», что приведёт к внутреннему отказу воспринимать реальность вне поля интересов **в принципе**. Человек, а тем более это критично для ребёнка, окружённый контекстным полем своих запросов, сделанных в прошлом, **просто перестаёт развиваться и расти**.

Говоря в системном плане – происходит атомизация и **инфантилизация** общества. Когда-то ребёнок, сделавший первый запрос в интернете в 12 лет, телесно повзрослеет, но, по сути, останется в том же двенадцатилетнем возрасте.

2. **Усугубление девиаций**. Во-вторых, пользователя, погружённого в цифровую реальность своего информационного пузыря, некому будет корректировать и ориентировать на созидательные вещи. При этом любые государственные программы, ориентированные на патриотизм или другие общественные ценности, будут абсолютно бесполезны по причине замкнутости недоразвитой детской психики внутри самого себя.

В процессе развития любой человек, естественным образом совершает ошибки, и, иногда, намеренно – вредные действия. Но, во все времена общество в лице окружения, так или иначе, корректировало, иногда «срамило» оступившегося, то есть воспитывало. Когда ребёнок понимал, что не прав, он испытывал стыд. Однако сегодня, когда почти каждый стал автономен внутри своего информационного пузыря, и общество **лишилось этих механизмов коррекции.**

В таком состоянии, когда **никакая корректировка** (воспитательная работа) извне невозможна, девиации в психике только усугубляются. И маркетинговая воронка играет здесь первую скрипку. Возможно, что он сначала лишь посмотрит лёгкий интересный голливудский фильм про мошенников, облапошивших банк. Затем контекстная реклама предложит подборку фильмов на данную тематику, включая такие опасные, отвратительные и социально вредные продукты типа «Волк с Уолл-Стрит» про «успешных трейдеров». Потом ещё пару занятных статеек о том, какие уловки используют мошенники, чтобы развести людей на деньги по телефону. Со временем стратегия мошенничества и обмана, покреплённая почерпнутыми мировоззренческими парадигмами «Бери от жизни всё», «Каждый сам за себя», «Выживает сильнейший/

умнейший/хитрейший», «Бедность не порок, а простое свинство» и другими, становится приемлемым, **«единственно возможным»** и очевидным способом взаимодействия с окружающим миром.

Психика пользователя в этом случае плавно проходит все ступени «окна Овертона», когда идея, которая прежде была немыслимой и категорически неприемлемой, постепенно становится разумной, популярной, и, в конце концов, – законной. Контекстная реклама – лишь один из инструментов насаждения противоестественных и антисоциальных норм.

3. Управление пользователем в обход его сознания.

В-третьих, необходимо понимать, что технологии безнравственны, будь-то DNS, cookies, контекстная реклама, или поисковая система. Каждая технология просто выполняет свой функционал, вопрос в том, кто и для чего их использует и какие критерии закладывает.

Ещё раз повторим, что сегодня речь идёт уже не только и не столько о том, чтобы затянуть пользователя в маркетинговую воронку, сколько о том, чтобы формировать привычки, образ жизни и мировоззрение человека, то есть в конечном счёте – выращивать своего «ручного потребителя». Потому-то многомиллионные штрафы за сбор данных о детях не останавливают глобальные корпорации (эти мизерные, в общем-то, штрафы для них – это всего лишь один из видов неизбежных мелких затрат, таких инвестиций в «потребителя Будущего»).

И здесь корпорации и IT-гиганты уже давно перешли красную черту дозволенного. Взяв на себя роль глобальных селекционеров, они потихоньку внедряют как норму стандарты цифрового, по сути, фашизма. Уничтожение человека, как человека в большом смысле, низведение его до уровня «квалифицированного потребителя», извращение его сознания посредством интернет-технологий на международном уровне должно быть приравнено к геноциду, т.е. к преступлению против человечества. И точно также за это должны судить на международном трибунале.

Воспитание человека – это прерогатива только государства и человеческого общества. Чтобы предотвратить установление фашистского цифрового режима, нужна общественная инициатива, но не абстрактная.

Нужны люди, понимающие и разбирающиеся как в технике, так и в социуме. И всем нам необходимо этому учиться. Это личное дело каждого из нас.

Когда во время Великой Отечественной войны фашисты по ночам сбрасывали на крыши наших городов бомбы-зажигалки, люди организовывали дежурства и тушили их. Ни у кого из этих людей не было убеждений, что тушить должен кто-то другой – пожарная команда, начальник или государство. Не возникало и вопросов о своей субъектности. Чего и нам желаем.

Литература:

1. Доктрина информационной безопасности Российской Федерации (принята Указом Президента Российской Федерации от 05.12.2016 года № 646) // электронный ресурс. – Режим доступа: http://www.kremlin.ru/acts/bank/41460
2. Бессонов Е.Г. Социально-технологические аспекты кибербезопасности// Наркомания как проблема социального здоровья молодёжи. Комплексные подходы к профилактике наркозависимости в подростковой среде. Материалы межрегиональной научно-практической конференции 19-21 апреля 2018 г. / Под редакцией П.А. Нуттунена. – СПб.: Выборг, 2018. – С. 8-12. - 66 с.
3. Мигулёва М.В. Киберпространство как фактор формирования социальных норм в молодёжной среде // Безопасность в сети Интернет: сб. материалов межрегиональных науч.-практ. конференций, 13.04.2017 и 8.11.2017 г./М.А. Горюнова, М.Б.Лебедева, М.И. Нефёдова. – Спб.: ЛОИРО, 2017 – С. 12-17. - 128 с.
4. Защита идеалов справедливости: новые формы и методы // электронный ресурс. – Режим доступа: http://center-si.com/analitics/zashhita-idealov-spravedlivosti-novye-formy-i-metody/
5. Контент как оружие социального инжиниринга // электронный ресурс. – Режим доступа: https://center-si.com/analitics/kontent-kak-oruzhie-socialnogo-inzhiniringa/
6. Информационно-просветительский фильм «Территория БезОпасности: Алгоритм Победы» // электронный ресурс. – Режим доступа: https://www.youtube.com/watch?v=HUedCmaXB4Y
7. Информационно-просветительский фильм «Территория БезОпасности. Отцы и дети» // электронный ресурс. – Режим доступа: https://www.youtube.com/watch?v=3LKqGt-MAqk
8. Сайт проекта «Территория БезОпасности» // электронный ресурс. – Режим доступа: http://киберстандарт.рф/

9. Материал РИА «Катюша». Ведите ваших деточек: Google и YouTube попались на сборе информации о детях без согласия родителей// электронный ресурс. – Режим доступа: http://katyusha.org/view?id=12652

10. Материал «Xakep.ru». Цифровой паноптикум. Настоящее и будущее тотальной слежки за пользователями // электронный ресурс. – Режим доступа: https://xakep.ru/2017/11/24/digital-panopticon/