Методические рекомендации для несовершеннолетних, родителей (законных представителей) несовершеннолетних по безопасному использованию сети Интернет в целях предотвращения преступлений, совершаемых с ее использованием как самими несовершеннолетними, так и в отношении них

ИРО
ИНСТИТУТ РАЗВИТИЯ ОБРАЗОВАНИЯ
Свердловской области

Министерство образования и молодежной политики Свердловской области
Государственное автономное образовательное учреждение
дополнительного профессионального образования Свердловской области
«Институт развития образования»
Центр воспитания и дополнительного образования

Методические рекомендации для несовершеннолетних, родителей (законных представителей) несовершеннолетних по безопасному использованию сети Интернет в целях предотвращения преступлений, совершаемых с ее использованием как самими несовершеннолетними, так и в отношении них

Екатеринбург 2022

ББК 74.200.5я81
М 54

Рецензенты:
Л. И. Долинер, доктор педагогических наук, профессор кафедры математики и информатики ГАОУ ДПО СО «Институт развития образования»;
А. А. Костылев, заместитель директора по праву МАОУ Гимназия № 86, г. Н. Тагил

Автор-составитель:
Е. Б. Стариченко, кандидат педагогических наук, доцент, директор регионального центра цифровой трансформации образования ГАОУ ДПО СО «Институт развития образования»

М 54 Методические рекомендации для несовершеннолетних, родителей (законных представителей) несовершеннолетних по безопасному использованию сети Интернет в целях предотвращения преступлений, совершаемых с ее использованием как самими несовершеннолетними, так и в отношении них / Министерство образования и молодежной политики Свердловской области, Государственное автономное образовательное учреждение дополнительного профессионального образования Свердловской области «Институт развития образования»; авт.-сост. Е. Б. Стариченко. – Екатеринбург: ГАОУ ДПО СО «ИРО», 2022. – 41 с.

В издании приводятся рекомендации по обеспечению защиты от отслеживания со стороны владельцев трекеров, построения ими поведенческого профиля и передачи его третьим лицам. Приводится объяснение необходимости этой деятельности, и даются рекомендации по настройке программного обеспечения на компьютерах и мобильных устройствах.

Утверждено Научно-методическим советом ГАОУ ДПО СО «ИРО» от 28.03.2022 № 4

ББК 74.200.5 я81

Оглавление

Введение

Интернет постоянно наблюдает за своими пользователями и посетителями. При этом практически каждый веб-ресурс делится данными, получаемыми от посетителей, с десятками третьих лиц. Большинство мобильных приложений делают то же самое. Многие из них собирают конфиденциальную информацию, такую как местоположение и записи звонков, даже если выключены в этот момент. Слежка и контроль проникают и в реальный мир. Торговые центры используют автоматические считыватели номерных знаков для отслеживания трафика через свои парковки, а затем делятся этими данными с правоохранительными органами. Предприятия, организаторы концертов и политические организации используют маяки Bluetooth и Wi-Fi для осуществления пассивного мониторинга людей. Розничные магазины используют распознавание лиц для идентификации клиентов, предотвращения краж и показа целевой рекламы.

Компании и рекламодатели, стоящие за этим наблюдением, технологии, которые им управляют, как правило, невидимы для пользователя. Мы видим только приложения, веб-страницы и рекламу, в то время как наблюдатели фиксируют практически все, что вы делаете. Они не всеведущи, но их очень много. Данные, которые они собирают и получают, не идеальны, но тем не менее весьма чувствительны.

Особенно это стоит понимать несовершеннолетним, которые значительную часть своей жизни проводят в Сети и часто не задумываются о том, как оставляемый ими информационный след и собираемая о них информация могут повлиять на их жизнь и судьбу через несколько лет.

Кто нас видит?

Крупнейшие компании в Интернете собирают огромные объемы данных, когда люди пользуются их услугами. «ВКонтакте» знает, кто ваши друзья, что вам нравится и что вы читаете в своей ленте новостей. «Яндекс» знает, что вы ищете в Сети и куда вы идете, когда перемещаетесь с помощью навигатора. «Сбербанк» знает, что вы покупаете и сколько на это тратите.

Данные, которые эти компании собирают с помощью своих собственных продуктов и услуг, называются «первичными данными». Данные иногда собираются в рамках явного или неявного договора: «Ставя галочку, вы принимаете условия Пользовательского соглашения и разрешаете нам получать доступ к информации на устройстве, обрабатывать персональные данные, данные геолокации и идентификации. Обратите

внимание, что обработка ваших персональных данных может не требовать вашего согласия, но вы имеете право возражать против такой обработки».

Кроме того, компании собирают столько же личной информации, если не больше, о людях, которые не используют их услуги. Например, о пользователях других веб-сайтов и приложений с помощью своих «пикселей конверсии». Или используя данные о местоположении для отслеживания посещений пользователями обычных магазинов. И тысячи других информационных брокеров[1], рекламодателей и других трекеров[2] скрываются на фоне нашего повседневного просмотра веб-страниц и использования устройств. Это называется «сторонним отслеживанием». Стороннее отслеживание гораздо сложнее идентифицировать, и его почти невозможно полностью избежать.

Что они знают?

Большинство пользователей знакомо с наиболее известными возможностями проникновения в частную жизнь своих устройств. Так, любой смартфон представляет собой карманный GPS-трекер, постоянно транслирующий свое местоположение через интернет. Устройства с камерами и микрофонами потенциально являются средством прослушивания. И риски реальны: некоторые крупные компании разрешали сотрудникам слушать аудио, записанное их домашними умными устройствами; фронтальные камеры ноутбуков использовались школами для контроля за учениками дома.

Но наиболее известные средства потенциального наблюдения не являются самыми распространенными и самыми угрожающими частной жизни. Камеры наших устройств крайне редко записывают и передают что-либо без явного намерения пользователя. И чтобы избежать нарушения законов, компании обычно воздерживаются от тайного прослушивания разговоров пользователей. Трекеры позволяют узнать гораздо больше из менее явных источников данных.

Наиболее распространенной угрозой нашей конфиденциальности является постоянное накопление данных о нашей жизни. Это включает в себя, например, историю просмотров, использование приложений, покупки и данные геолокации, места, где мы расплачиваемся банковскими

---

[1] Информационные брокеры (брокеры данных) – это компании, которые занимаются сбором и зарабатывают на продаже персональных данных.

[2] Трекер – технология отслеживания посещаемых интернет-ресурсов. Когда вы посещаете сайт, трекер сохраняется на вашем компьютере.

картами, суммы, которые мы тратим. Эти, казалось бы, несвязанные события и действия могут быть объединены в весьма интересное целое. Трекеры собирают данные о наших кликах, показах, касаниях и перемещениях в поведенческие профили, которые могут выявить политическую принадлежность, религиозные убеждения, расу и этническую принадлежность, уровень образования, уровень дохода, покупательские привычки, а также физическое и психическое здоровье.

Поведенческая реклама – это использование данных о поведении пользователей для предсказания того, что им нравится, как они думают и что они, вероятно, купят. Пока еще мы видим довольно большой разброс рекламных предложений от удивительно точных до совершенно нецелевых. Но мы видим эти предложения везде, где бы в интернете мы ни оказались, в том числе и на разных устройствах. А точность – вопрос времени и объема собранных о нас данных. Но независимо от того, верны ли выводы трекеров или нет, данные, которые они собирают, представляют собой вторжение в частную жизнь, и решения, которые принимаются на основе этих данных, могут нанести ощутимый вред.

Данные и люди

Большинство трекеров предназначены для создания профилей реальных людей. Для этого трекер использует идентификаторы, которые помогают устанавливать эту связь. Например, собранные данные могут соотноситься с конкретным устройством или браузером, которые, в свою очередь, могут быть соотнесены с одним человеком или с семьей.

Веб-идентификаторами могут служить cookies (печеньки), IP-адрес, MAC-адрес, состояние TLS (Transport Layer Security). Идентификаторами телефонов являются номер телефона, номер IMSI и IMEI, MAC-адрес, рекламный идентификатор. Также к средствам идентификации следует отнести номерной знак автомобиля, лицо человека, номер банковской карты. Конечно, существует больше способов идентификации пользователей, чем мы можем охватить и даже представить, и новые будут появляться с развитием технологий.

Идентификаторы в интернете

Браузеры являются основным способом взаимодействия большинства людей с интернетом. Каждый раз, когда вы посещаете веб-сайт, код на этом сайте приводит к тому, что ваш браузер сделает десятки скрытых запросов. Каждый запрос содержит информацию, которая может быть использована для отслеживания.

Взаимодействие между браузером и сервером веб-сайта происходит в форме HTTP-запроса. Браузер запрашивает у веб-сервера контент, отправляя ему URL-адрес (рис. 1). Веб-сервер может ответить контентом, таким как текст или изображение, или подтверждением того, что он получил ваш запрос. Он также может отвечать с помощью файла cookie, который содержит уникальный идентификатор для отслеживания.

Каждый веб-сайт, который вы посещаете, запускает десятки различных запросов. URL-адрес, который вы видите в адресной строке вашего браузера, является адресом для первого запроса, но множество других запросов выполняются в фоновом режиме. Их можно использовать для загрузки изображений, кода и стилей или просто для обмена данными.

Рис. 1. Части URL-адреса

Сам URL-адрес содержит несколько различных блоков информации: протокол (указывает на правила обмена информацией); доменное имя (домен, например, irro.ru) указывает браузеру, к какому серверу подключиться; путь к фрагменту кода, исполняемому браузером; параметры, содержащие дополнительную информацию о запросе, включая запросы, сделанные пользователем, контекст страницы и идентификаторы отслеживания.

После того, как запрос покидает компьютер, он перенаправляется маршрутизатором интернет-провайдеру, который отправляет его через серию промежуточных станций маршрутизации. В итоге запрос поступает на сервер, указанный доменом, который может решить, как на него реагировать.

URL-адрес – это не все, что отправляется на сервер. Существуют также заголовки HTTP, которые содержат дополнительную информацию о запросе, такую как язык и настройки безопасности вашего устройства, «ссылающийся» URL-адрес и файлы cookie. Например, заголовок User-Agent определяет тип, версию и операционную систему браузера. Существует также низкоуровневая информация о соединении, включающая IP-адрес и состояние общего шифрования. Некоторые запросы содержат еще более подробную информацию в виде данных POST. Запросы POST – это способ обмениваться фрагментами данных, которые слишком велики, чтобы поместиться в URL-адресе. Они могут содержать практически все что угодно (рис. 2).

Некоторая часть этой информации, такая как данные URL и POST, специально адаптирована для каждого отдельного запроса; другие части, такие как IP-адрес и любые файлы cookie, автоматически отправляются компьютером. Почти все это можно использовать для отслеживания.

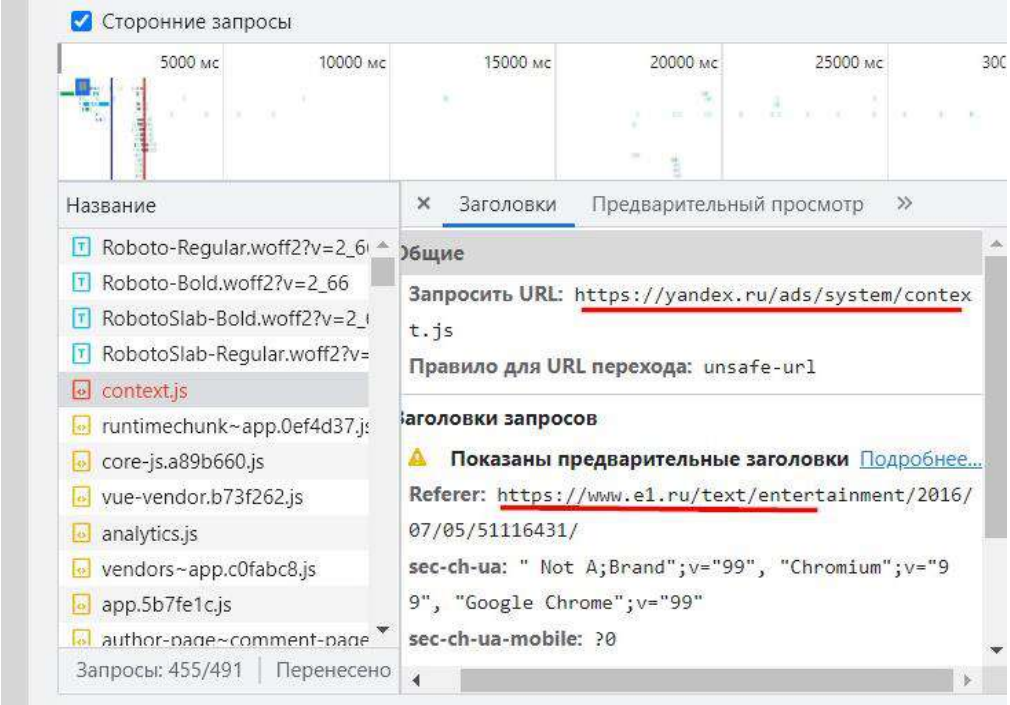

Рис. 2. Данные, включенные в фоновый запрос.
На изображении, хотя пользователь перешел на www.e1.ru,
страница инициирует сторонний запрос на yandex.ru в фоновом режиме

Все основные браузеры имеют режим разработчика, который позволяет видеть, что скрыто от глаз пользователя, включая запросы, поступающие с определенной вкладки. Чаще всего доступ к интерфейсу можно получить с помощью комбинации Crtl + Shift + I. На вкладке «Сеть» есть журнал всех запросов, сделанных определенной страницей, и можно кликнуть по каждому из них, чтобы увидеть, куда он идет и какую информацию содержит.

Идентификационная информация передается автоматически вместе с каждым запросом. Происходит это по технической необходимости, как в случае с IP-адресами, либо умышленно, как в случае с файлами cookie. Трекерам не нужно делать ничего специально для сбора информации, все уже заложено в механизмы обмена информацией (рис. 3).

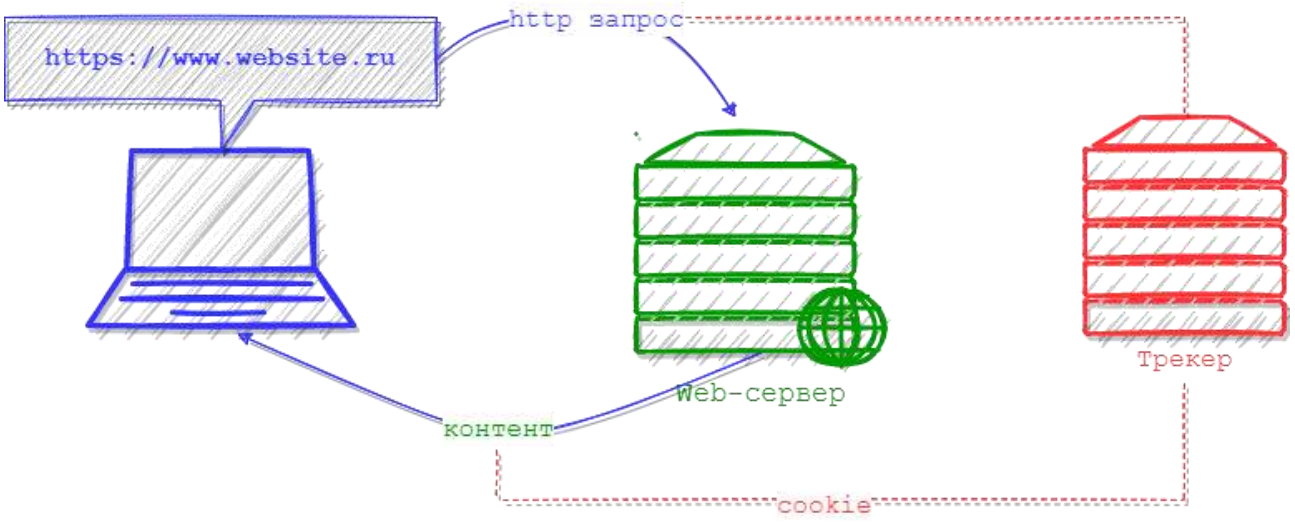

Рис. 3. Каждый раз, когда вы заходите на веб-сайт, вводя URL-адрес или переходя по ссылке, ваш браузер делает запрос на сервер этого веб-сайта. Благодаря коду, размещенному на загружаемой веб-странице, он также может делать десятки или сотни запросов другим серверам, которые могут отслеживать вас

Cookie

Наиболее распространенным инструментом для стороннего отслеживания является файл cookie. Он представляет собой небольшой фрагмент текста, который хранится в памяти браузера и связан с определенным доменом. Файлы cookie были придуманы для того, чтобы помочь владельцам веб-сайтов определить, посещал ли пользователь их сайт раньше. В основном они используются для запоминания таких полезных вещей, как данные для входа в учетную запись или содержимое корзины на сетевой торговой площадке. Однако именно это делает их прекрасным инструментом для отслеживания поведения.

Механизм их работы прост. При первом обращении к домену, например www.e1.ru, сервер присоединяет к своему ответу заголовок Set-Cookie. Это дает команду браузеру сохранять получаемые cookie. После этого каждый раз, когда браузер обращается к https://www.e1.ru/, он отправляет файл cookie, который получил при первом посещении (рис. 4). Таким образом, каждый раз, когда сайт получает запрос, он знает, от какого пользователя или устройства он исходит.

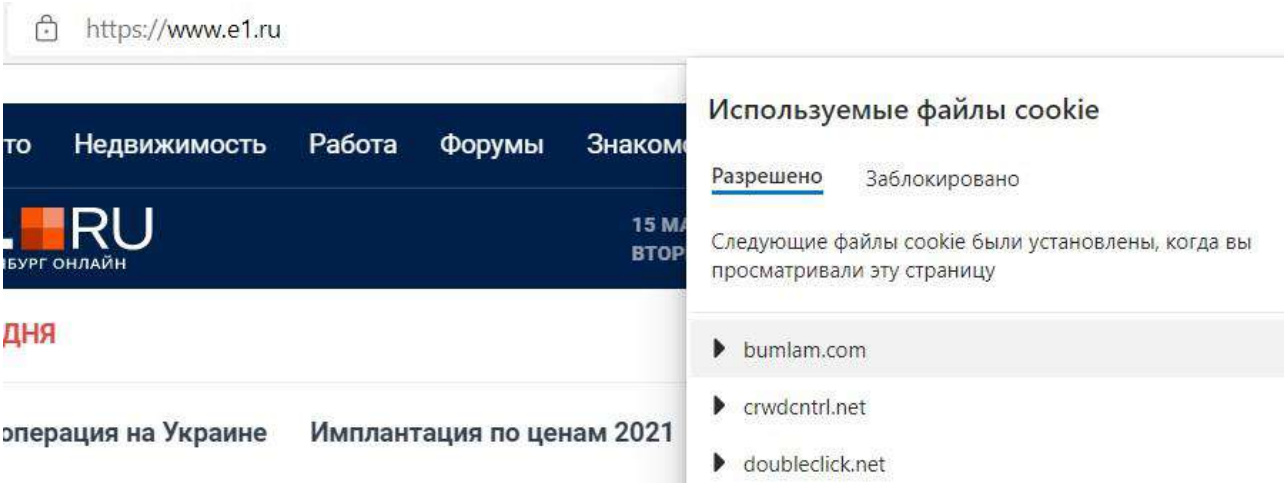

Рис. 4. Посторонние ресурсы, cookie которых получены браузером при посещении сайта

Не каждый файл cookie является трекером. Как правило, это просто средство обмена информацией между браузером и веб-сайтом. Оно позволяет вам продолжить работать с сайтом с того состояния, в котором вы оставили его при предыдущем посещении. Например, вернуться в интернет-магазин и продолжить покупки. Тем не менее они позволяют передавать информацию для отслеживания, и это является их самым неприятным применением.

Пользователи имеют возможность контролировать процесс обработки и сохранения файлов cookie браузером. Их загрузку можно отключать, сохраненные файлы можно автоматически удалять при выходе, а с недавних пор можно ограничивать доступ к сторонним файлам cookie. Это уже имеет положительные результаты – трекеры перестают использовать исключительно файлы cookie для идентификации пользователей.

IP-адрес

Каждый запрос, который вы делаете через интернет, содержит ваш IP-адрес – идентификатор, уникальный для вашего устройства. Он меняется каждый раз, когда вы переходите в новую сеть (например, с работы в кафе), и даже может меняться, когда вы остаетесь в одной и той же сети.

Существует две версии IP-адресов – IPv4 и IPv6. IPv4 был разработан на заре интернета и использует 32-разрядное адресное пространство, которое предоставляет 4 294 967 296 уникальных адресов (2^{32}). При этом в мире насчитывается более 22 миллиардов подключенных к сети устройств и более 70 % интернета использует IPv4. Это стало возможно благодаря тому, что IPv4-адреса, используемые пользовательскими

устройствами, постоянно переназначаются. Когда устройство подключается к сети, его интернет-провайдер предоставляет ему аренду IP-адреса. Это позволяет устройству использовать один адрес в течение нескольких часов или дней. Когда срок аренды истекает, интернет-провайдер может принять решение о продлении аренды или предоставлении нового IP-адреса. Если устройство остается в одной и той же сети в течение длительного времени, его IP-адрес может меняться каждые несколько часов или не меняться в течение нескольких месяцев.

Адреса IPv6 не имеют проблемы дефицита. Адрес представляет собой восемь 16-битных блоков, разделенных двоеточиями: 2dfc:0:0:0:0217:cbff:fe8c:0. Общее количество IPv6 адресов, возможных для распределения, может составить в общей сложности 2^{128} (приблизительно 340 282 366 920 938 000 000 000 000 000 000 000 000), что сильно превышает количество устройств, способных сегодня подключиться к интернету. Их не нужно менять, но благодаря техническому стандарту большинство устройств генерируют новый, случайный IPv6-адрес каждые несколько часов или дней. Это означает, что адреса могут использоваться для краткосрочного отслеживания, но не могут являться долгосрочными идентификаторами [1].

Сами по себе IP-адреса не являются хорошими идентификаторами, но при достаточном количестве данных трекеры могут использовать их для создания долгосрочных профилей пользователей, в том числе и сопоставления отношений между устройствами [2]. IP-адрес можно скрыть, используя VPN-сервер.

Состояние TLS

Сегодня значительная часть трафика в интернете шифруется с помощью Transport Layer Security, или TLS. Каждый раз, когда вы подключаетесь к URL-адресу, который начинается с «https://», вы подключаетесь с помощью TLS. Шифрованное соединение, которое предоставляют TLS и HTTPS, гарантирует, что данные не перехватываются или не изменяются в процессе передачи.

Тем не менее это открывает новые способы идентификации пользователей с помощью идентификаторов сеансов TLS. При подключении к серверу по протоколу HTTPS браузер запускает новый сеанс TLS, и идентификатор сеансов помогает ускорить процедуру шифрованного соединения.

Настройка сеанса включает в себя ресурсоемкую криптографическую работу, поэтому сервер, вместо того чтобы выполнять полную криптографическую процедуру с браузером, при повторном подключении может отправить сеансовый билет. В следующий раз, когда вы подключитесь к тому же серверу, браузер отправит билет, позволяя обеим сторонам пропустить полную процедуру. И единственная проблема в этом механизме в том, что сеансовый билет может быть использован трекерами в качестве уникального идентификатора.

Как и IP-адреса, сеансовые билеты всегда уникальны и доступны, если браузер не настроен на их отклонение. Серверы обычно настраивают срок хранения сеансовых билетов до недели, но возможности браузера позволяют удалять их раньше.

Отслеживание мобильных устройств

Смартфоны, планшеты и читалки электронных книг тоже обычно имеют браузеры. И эти устройства также подвержены отслеживанию. Учитывая их персональный характер, это имеет более серьезные последствия для пользователя.

Есть у мобильных устройств и отличительные особенности. Пользователям необходимо войти в систему с помощью учетной записи, например Apple или Google. Это связывает идентификаторы устройств с ними и облегчает профилирование поведения пользователей. Например, благодаря вашему смартфону Google прекрасно знает ваш домашний адрес, место работы, что вы ищете в интернете и какие приложения используете. И использует это для демонстрации вам рекламы с учетом вычисленных им ваших интересов (таргетинга).

Большинство людей значительную часть времени используют на смартфоне не браузер, а мобильные приложения. Трекеры в приложениях не имеют доступа к файлам cookie, но могут получать уникальные идентификаторы устройства, которые удобно использовать для отслеживания.

В мобильной среде значительная часть отслеживания происходит с помощью сторонних комплектов для разработки программного обеспечения, или SDK. Пакет SDK – это библиотека кода, которую разработчики приложений могут включить в свои приложения. Разработчик приложений, который хочет использовать стороннюю аналитическую службу или показывать стороннюю рекламу, загружает фрагмент кода, например, из «Яндекса» или VK. Затем он включает этот код в опубликованную версию

своего приложения. В результате сторонний код имеет доступ ко всем данным, которые доступны приложению, например, к местоположению, контактам или камере.

Браузеры умеют накладывать дополнительные ограничения на сторонний контент, например, блокировать доступ к хранилищу браузера. В мобильных приложениях этой возможности нет. Вы не можете предоставить право на доступ к ресурсам смартфона приложению, не предоставив такое же право всему стороннему коду, выполняемому внутри него.

Телефонные номера

Номер телефона является одним из наиболее известных уникальных числовых идентификаторов и одним из самых простых для понимания. Каждая комбинация цифр уникальна для конкретного устройства и меняется довольно редко. Для пользователей создаются условия, в которых они вынуждены делиться своими номерами телефонов по целому ряду причин (например, регистрация на каком-либо ресурсе в Сети, проверка учетной записи, оплата через интернет-эквайринг, участие в программе лояльности магазина и т. п.). С помощью этих механизмов брокеры данных собирают и продают номера телефонов, а мы получаем рекламные сообщения и звонки.

Но у приложений практически нет шансов получить доступ к телефонному номеру. На Android телефонные номера доступны приложениям только при предоставлении специального разрешения [16]. iOS полностью запрещает доступ приложениям к номеру телефона пользователя [9]. Телефонные номера уникальны и постоянны, но недоступны сторонним трекерам в большинстве приложений.

Идентификаторы оборудования

Каждому устройству, которое может подключаться к мобильной сети, присваивается уникальный идентификатор – международный номер идентификации абонента (IMSI) [10]. Номера IMSI присваиваются мобильными операторами и хранятся на SIM-картах. Изменить их без замены карты нельзя. Это делает их прекрасным инструментом отслеживания.

Каждое мобильное устройство имеет международный идентификационный номер мобильного оборудования (IMEI), «зашитый» в аппаратное обеспечение. Вы можете изменить SIM-карту и номер телефона, но не можете изменить IMEI, не купив новое устройство [10].

Номера IMSI передаются оператору сотовой связи каждый раз, когда устройство подключается к узлу связи, что происходит постоянно, особенно при движении. Когда вы прогуливаетесь по городу, ваш телефон отправляет запросы на близлежащие узлы, чтобы получить информацию о состоянии сети. Оператор может использовать эту информацию для отслеживания местоположения телефона (и ваше вместе с ним). Это не совсем стороннее отслеживание, так как оно осуществляется оператором сотовой связи, с которым у вас заключен договор, но многие пользователи не осознают, что это происходит.

Приложения, работающие на смартфоне, практически не могут получать доступ к номерам IMSI и IMEI, этот процесс затруднен теми же механизмами, что и доступ к номеру телефона. Мобильные операционные системы блокируют доступ к идентификаторам. Как и номера телефонов, номера IMSI и IMEI уникальны и постоянны, но недоступны для трекеров.

Рекламные идентификаторы

Рекламный идентификатор – это длинная случайная строка букв и цифр, которая однозначно идентифицирует мобильное устройство. Рекламные идентификаторы не являются частью технических протоколов, но встроены в операционные системы iOS и Android. Они аналогичны файлам cookie в интернете. Рекламные идентификаторы хранятся на телефоне и передаются трекерам в разных приложениях. Идентификаторы объявлений несут единственную функцию – помочь рекламодателям связать активность пользователей с приложениями на устройстве.

В отличие от номеров IMSI или IMEI, рекламные идентификаторы можно изменить или полностью отключить [11], но по умолчанию они включены и доступны для всех приложений без специальных разрешений. И создатели мобильных операционных систем поощряют разработчиков приложений использовать рекламные идентификаторы для формирования поведенческого профиля вместо других идентификаторов, мотивируя это тем, что пользователям предоставляется больше контроля над тем, как они отслеживаются. Однако на практике, даже если пользователь вручную сбросит свой рекламный идентификатор, трекеры смогут идентифицировать их с помощью IP-адреса или хранилища в приложении. Например, платформа Android не имеет механизмов, запрещающих разработчикам подобную деятельность. Согласно исследованию, проведенному Международным институтом компьютерных наук, более половины приложений, размещенных в Google Play, ведут незаконную слежку за пользователями [12].

Рекламные идентификаторы уникальны и доступны для всех приложений по умолчанию. Они хранятся до тех пор, пока пользователь вручную их не сбросит. Это делает их очень привлекательными для скрытых трекеров.

MAC-адрес

Каждое устройство, подключаемое к интернету, имеет аппаратный идентификатор, называемый Media Access Control (MAC-адрес). Они используются всеми видами устройств, но риски нарушения конфиденциальности, связанные с ними, выше на мобильных устройствах. Веб-сайты и серверы, с которыми вы взаимодействуете через интернет, не имеют доступа к MAC-адресу, но любые сетевые устройства, через которые вы к нему подключаетесь, его видят. Более того, не нужно даже подключаться к беспроводной сети, чтобы она увидела ваш MAC-адрес, достаточно просто оказаться в зоне ее действия.

Чтобы найти ближайшие устройства Bluetooth и сети Wi-Fi, смартфон (планшет, ноутбук) постоянно посылает короткие радиосигналы, называемые зондовыми запросами. Каждый запрос содержит уникальный MAC-адрес сетевого адаптера устройства. Если устройство оказывается в зоне действия беспроводной сети, она получит запрос и отправит обратно свой ответ, адресованный MAC'у вашего устройства, с информацией о том, как вы можете к ней подключиться.

Но другие устройства в зоне распространения зондовых запросов также могут видеть и перехватывать их. Это означает, что компании могут создавать беспроводные «маяки», которые молча слушают MAC-адреса вокруг себя. Эту информацию можно использовать для отслеживания движения конкретных устройств. Маяки часто устанавливаются на предприятиях, в магазинах и на общественных мероприятиях. Имея достаточное количество маяков в достаточном количестве мест, компании могут отслеживать перемещение пользователей, могут определить, когда два человека находятся в одном и том же месте, и использовать эту информацию для построения социальных графов [3] и персонализации рекламы [23].

Предотвращать такую форму отслеживания можно с помощью рандомизации MAC-адресов. Вместо того, чтобы делиться своим истинным уникальным MAC-адресом в зондовых запросах, смартфон может каждый раз создавать случайный MAC-адрес для текущей передачи. Это делает невозможным связывать один запрос с другим или с конкретным устройством. Последние версии мобильных операционных систем по умолчанию

включают рандомизацию MAC-адресов. Этот механизм не работает на ноутбуках и старых телефонах.

Аппаратные MAC-адреса глобально уникальны. Они постоянны, не изменяются в течение жизни устройства. Они недоступны для трекеров в приложениях, но доступны для беспроводных маяков. Однако, поскольку многие устройства теперь умеют генерировать случайные MAC-адреса, они становятся менее надежным идентификатором для пассивного отслеживания.

Идентификаторы реального мира

Многие идентификаторы электронных устройств могут быть сброшены, запутаны или отключены пользователем. В реальном мире это сделать сложнее. За нечитаемый номер автомобиля можно получить штраф; практически невозможно изменить биометрические идентификаторы, такие как лицо, голос, походка, отпечатки пальцев.

Номерные знаки

Каждый автомобиль должен иметь номерной знак, который привязан к физическому лицу (человеку) или организации. И они являются прекрасным идентификатором для отслеживания. Их легко считывать и распознавать, незаконно менять, и они находятся там же, где автомобиль владельца, часто вместе с владельцем.

Автоматические считыватели номерных знаков представляют собой специальные камеры, которые могут автоматически идентифицировать и записывать номерные знаки проезжающих автомобилей [14]. Они могут быть установлены на перекрестках, парковках торговых центров, на других транспортных средствах. Частные компании управляют сетью считывателей и используют их для накопления данных о местоположении автомобилей, продают эти данные другим предприятиям.

Отслеживания с помощью автоматических считывателей невозможно избежать, передвигаясь на собственном автомобиле. Скрывать или менять номерной знак незаконно, а избежать самих устройств чрезвычайно трудно. Номерные знаки уникальны, доступны любому, кто может видеть транспортное средство, и чрезвычайно стойки. Они являются идеальными идентификаторами для сбора данных о транспортных средствах и их водителях как для правоохранительных органов, так и для сторонних трекеров.

Биометрия лица

Лица – это еще один класс идентификаторов, привлекательных для сторонних трекеров. Лица уникальны и довольно неудобны для изменения. К счастью, пока не является незаконным скрывать свое лицо, но чаще всего это просто непрактично.

Лицо каждого человека уникально, доступно и стойко. Тем не менее современное программное обеспечение для распознавания лиц иногда путает одно лицо с другим. Алгоритмы более склонны к совершению такого рода ошибок при идентификации детей, женщин и пожилых людей.

Распознавание лиц уже получило широкое распространение, но мы только начинаем ощущать степень его воздействия. Камеры распознавания лиц уже есть в магазинах, на улицах и даже могут быть закреплены на компьютерных очках. Без строгих правил конфиденциальности у обычных людей практически не будет возможности бороться с повсеместным отслеживанием и профилированием с помощью распознавания лиц. Пока помогают маски и капюшоны.

Банковские карты

Банковские карты являются еще одним отличным долгосрочным идентификатором. И хотя они могут быть заблокированы, большинство людей нечасто меняют карты. Кроме того, номера банковских карт привязаны к физическим лицам, иногда организациям, и любой, кто получает номер вашей карты в рамках транзакции, также получает информацию о вас.

В каждой транзакции по банковской карте участвует большое количество скрытых третьих сторон. Если вы покупаете молоко в магазине у дома и расплачиваетесь картой, то информация о вас и вашей покупке проходит через платежный процессор, который предоставляет магазину услуги по обработке карт. Транзакция должна быть проверена банком магазина и банком, выдавшим вашу карту. Платежная система может нанимать другие компании для проверки своих транзакций, и все эти компании будут получать информацию о том, что вы купили молоко. Банки и другие финансовые учреждения регулируются стандартами безопасности данных. Однако другие финансовые технологические компании, такие как платежные процессоры и агрегаторы данных, зарегулированы заметно меньше.

Связывание идентификаторов

Часто трекер не может полагаться на один идентификатор для обеспечения стабильной связи с пользователем. IP-адреса меняются, люди очищают файлы cookie, сбрасывают рекламные идентификаторы, а более опытные используют разные номера телефонов и адреса электронной почты для разных задач, разделяя тем самым части своей личности. Чтобы избежать потери пользователя, трекеры объединяют несколько идентификаторов для создания единого профиля. Так они с меньшей вероятностью потеряют его след при изменении того или иного идентификатора, и со временем они могут связать старые идентификаторы с новыми. Если пользователь очищает файлы cookie на компьютере, но его IP-адрес не меняется, то связать новый файл cookie со старым очень просто. Если пользователь переходит из одной сети в другую, но использует один и тот же браузер, то он может связать старый сеанс с новым. Если блокируются чужие cookie, трекеры могут использовать сторонний обмен файлами cookie в сочетании с данными сеанса TLS для создания долгосрочного профиля поведения пользователя. В этой игре трекеры имеют технологические преимущества перед отдельными пользователями.

Рекламные сети

Онлайн-реклама является одним из основных потребителей сбора данных. Одна рекламная сеть показывает рекламу на нескольких веб-сайтах. Владелец сайта, работающий с сетью, должен разместить на своем веб-сайте небольшой фрагмент кода, который загрузит объявление с сервера. Запрос к рекламному серверу происходит каждый раз, когда пользователь посещает один из сотрудничающих сайтов. Это позволяет ему устанавливать сторонние cookie в браузерах пользователей и отслеживать их активность в сети. Аналогичным образом рекламный сервер может предоставлять разработчикам мобильных приложений пакет средств разработки программного обеспечения (SDK) для размещения рекламы. Всякий раз, когда пользователь открывает приложение, использующее SDK рекламного сервера, оно отправляет ему запрос, содержащий рекламный идентификатор, что позволяет серверу фиксировать действия пользователя в приложениях.

Пиксели-аналитики

Код отслеживания часто не связан с чем-либо видимым для пользователей, например с рекламной вставкой. Часто отслеживание происходит через микроскопические изображения размером 1x1 пиксель, которые существуют только для того, чтобы вызывать запросы к трекерам. Эти «пиксели отслеживания» используются многими интеграторами данных, включая «Яндекс», VK и другие.

Владельцы веб-сайтов устанавливают пиксели отслеживания третьей стороны в обмен на доступ к данным, которые она собирает. Например, информацию о том, какие люди посещают сайт, какова эффективность кликов собственных сторонних объявлений.

Медиаблоки

Иногда сторонние трекеры обеспечивают контент, который пользователи согласны и хотят видеть. Его встраивание – распространенное явление для блогов и медиасайтов. Очень часто можно встретить видеоплееры для YouTube, Vimeo, Streamable, аудиовиджеты для сервисов потоковой передачи подкастов. Такие плееры почти всегда работают внутри IFrames, имеют доступ к локальному хранилищу и возможность запуска произвольного кода JavaScript. Благодаря этому они очень подходят для отслеживания пользователей.

Социальные сети часто предоставляют веб-сайтам различные услуги, мотивируя их увеличением трафика и присутствием в социальных сетях. Но кнопки и виджеты социальных сетей можно использовать для отслеживания так же, как и пиксели: кнопка на самом деле является встроенным изображением, которое вызывает запрос к серверу.

Крупные интернет-компании предлагают услуги по управлению учетными записями, предоставляя сервисы единого входа. Это удобный сервис, так как с его помощью веб-сайты и приложения могут перепоручить управление учетными записями пользователей. Сами пользователи могут с помощью одной пары логин/пароль входить на разные ресурсы и реже проходить авторизацию. Но, как мы уже понимаем, за это удобство потребители расплачиваются тем, что позволяют сервису единого входа отслеживать активность пользователей на всех ресурсах, которыми они пользуются. И это более надежные трекеры, чем пиксели или виджеты, потому что они заставляют людей подтверждать свою личность.

Существует еще один интересный инструмент сбора данных о действиях пользователя. Сценарии воспроизведения сеансов владельцы веб-

сайтов или приложений устанавливают, чтобы записывать, как пользователи взаимодействуют с сервисом. Они похожи на экранные записи. Вебсайт может видеть все, что вы делаете: от движений и кликов мыши до символов, которые вы набираете. В том числе и тех, которые вы вводите, но не отправляете [8]. При этом пользователи часто даже не знают, что их действия записываются и передаются третьим лицам.

Все это создает риск того, что конфиденциальные и персональные данные будут записаны и переданы без ведома владельца. Порой пользователь может провести тонкую настройку и определить данные как запрещенные к передаче, но это весьма кропотливая и трудоемкая работа. В результате конфиденциальные данные попадают в записи, а поставщики услуг воспроизведения сеансов часто не могут должным образом их защитить.

Брокеры данных

Брокеры данных, или информационные брокеры, – это компании, которые собирают, агрегируют, обрабатывают и продают данные. Они работают вне поля зрения обычных пользователей, но в центре экономики обмена данными. Брокеры данных не имеют прямых отношений с пользователями, и люди, сведения о которых они продают, могут не знать об их существовании. Брокеры покупают данные у различных компаний и частных продавцов, например, финансовых, медицинских, операторов сотовой связи и интернета вещей. Эти данные они агрегируют и продают их или услуги на их основе банкам, рекламодателям, агентствам по недвижимости, компаниям по исследованию рынка, сервисам по найму или другим брокерам данных. Или используют их для сбора своих собственных поведенческих профилей, которые затем уже продают или используют, например, в политических или социальных кампаниях.

Потребители данных

Наиболее известными и распространенными потребителями данных являются рекламодатели. Таргетированная (целевая) реклама позволяет им охватить пользователей на основе множества признаков, таких как демография, возраст, социальный профиль и другие. Поведенческая реклама – это подмножество целевой рекламы, которое использует данные о прошлом поведении пользователей для персонализации рекламы.

Но рекламщики не единственные организации, которые пытаются извлечь выгоду из сбора данных и построения профилей пользователей.

Агрегированные личные данные используются для построения «портретов» миллионов потенциальных избирателей и последующего проведения политических кампаний. Например, используя данные о местоположении мобильного телефона, можно определить группу посещающих церкви, а затем сформировать для них целевую рассылку с учетом вероисповедания. Группы, выступающие против абортов, используют эту технологию для формирования целевой рекламы для женщин, посещающих соответствующие клиники. И это не единичные случаи. Некоммерческие организации, которые полагаются на пожертвования, покупают данные, чтобы сузить круг потенциальных жертвователей; многие политики используют открытые данные регистрации избирателей для их таргетинга.

Как с этим жить?

Можно спокойно мириться с тем фактом, что мы всегда находимся под наблюдением. На улице и в общественных местах мы постоянно попадаем в объективы камер наблюдения; используя компьютеры и мобильные телефоны, мы получаем рекламу, устройства рассылают без нашего ведома информацию о звонках, контактах и местоположении. За это мы получаем удобные сервисы, позволяющие принимать правильные и своевременные решения (например, сервисы прогноза погоды или городских пробок). Мы живем в новом мире, и все это – неотъемлемые его части.

Но порой стоит задумываться о том, как и какие сведения о вас попадают к неизвестным людям и как они могут ими распорядиться. Далеко не всех устраивает, что личная информация обменивается и продается без ведома владельца; кто-то не склонен делиться своим местоположением с неограниченным кругом лиц; кто-то опасается, что данные, собранные информационными брокерами, окажутся в недобросовестных руках; или отслеживание может быть просто постоянной неприятностью, которая создает смутное чувство беспокойства. И возможно, вы захотите ограничить отслеживание, чтобы избежать персонализированной или манипулятивной рекламы.

Правда, избежать его трудно. Все имеющиеся в арсенале способы наблюдения и контроля предусмотреть и предотвратить непросто. Все зависит от того, сколько усилий и времени вы готовы потратить на защиту своей конфиденциальности. Небольшие настройки программного обеспечения, штатные инструменты операционных систем и браузеров могут серьезно сократить объем данных, которые собирают трекеры.

Настройка браузера

Существует несколько способов ограничить доступ к отслеживанию в глобальной сети. Встроенные инструменты современных браузеров позволяют довольно сильно осложнить жизнь коду, отслеживающему вашу жизнь.

Мы уже обсуждали, что при каждом входе сайт запрашивает информацию у вашего браузера. Некоторые данные необходимы для правильного отображения сайта: например, сведения о языке устройства помогают автоматически выбрать подходящую локализацию, о типе (компьютер, мобильный телефон) – открыть более удобную мобильную версию сайта, если вы пользуетесь смартфоном, и т. д. Но собранная информация работает и против вас. Ее используют для сбора статистики, для продажи, например, рекламным агентствам, интернет-магазинам, политикам и т. д. И чем больше информации о вас соберут, тем более уникальным пользователем интернета вы становитесь. И это тот случай, когда быть уникальным плохо.

Снижение собственной уникальности

Увидеть, какую информацию передает о вас браузер, можно, посетив такие ресурсы, как https://coveryourtracks.eff.org, https://www.deviceinfo.me, https://ipper.ru. Это лишь некоторые примеры. Совокупность такой информации называется отпечатком браузера. Сбор сведений осуществляется сразу при подключении к сайту, так как браузер отправляет данные при запросе веб-страницы. Для оценки текущего состояния приватности (наличия уникального отпечатка) достаточно открыть настройки браузера и посмотреть, сколько всего разрешено. Но воспользуемся сетевыми инструментами.

С помощью ресурса https://coveryourtracks.eff.orgполучим отпечаток своего браузера и изучим его (рис. 5).

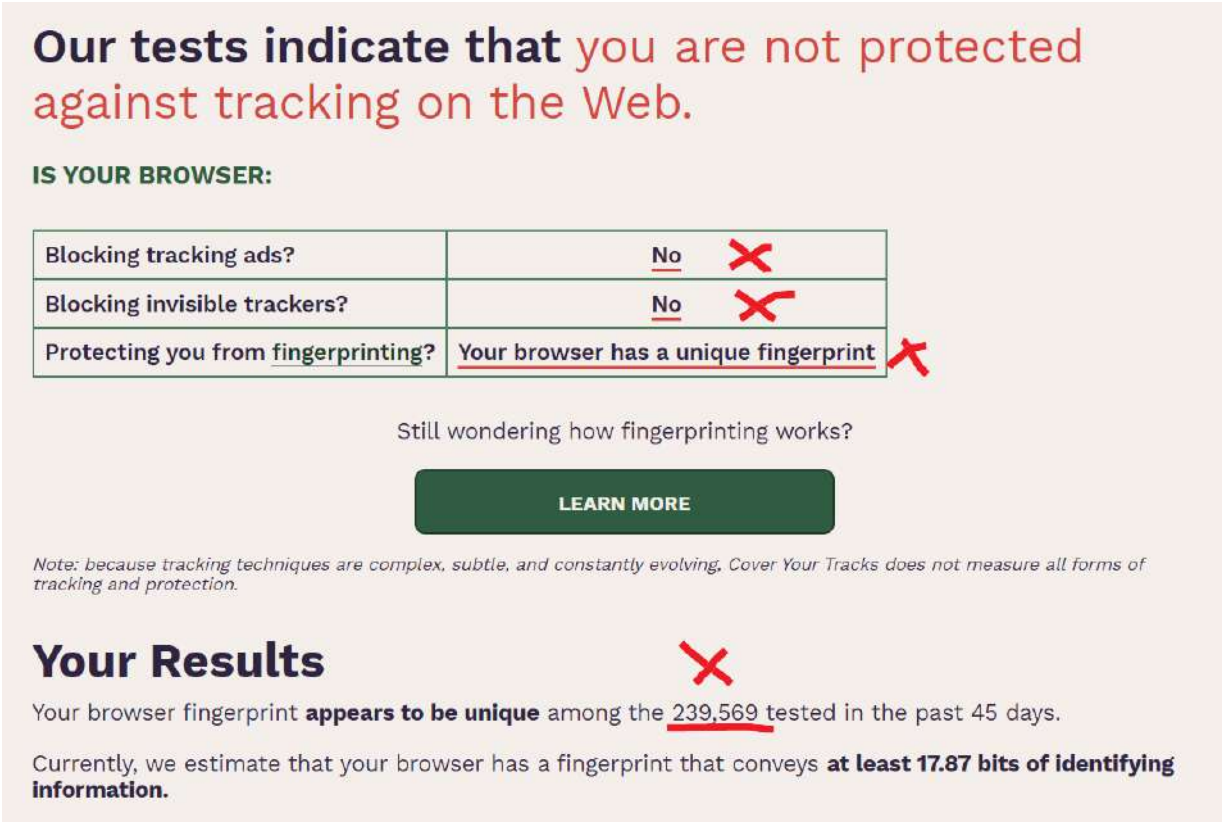

Рис. 5. Демонстрация уникальности отпечатка браузера. Красным обозначены позиции, требующие внимания: трекеры браузером не блокируются, у него есть отпечаток, уникальный среди почти 240 000 протестированных браузеров

Попробуем настроить браузер на обеспечение достаточного уровня приватности, помня, что полная анонимность тоже является отличительным признаком и привлекает еще больше внимания к вам.

У всех браузеров есть режим инкогнито, который обеспечивает защиту конфиденциальности только от других пользователей устройства, с которого вы выходите в интернет. В Chrome этот режим включается в правом верхнем углу экрана (три точки, расположенные вертикально). Если их нажать, выпадает меню, где надо выбрать «Новое окно в режиме инкогнито». Также можно нажать комбинацию клавиш «Ctrl + Shift + N» (рис. 6).

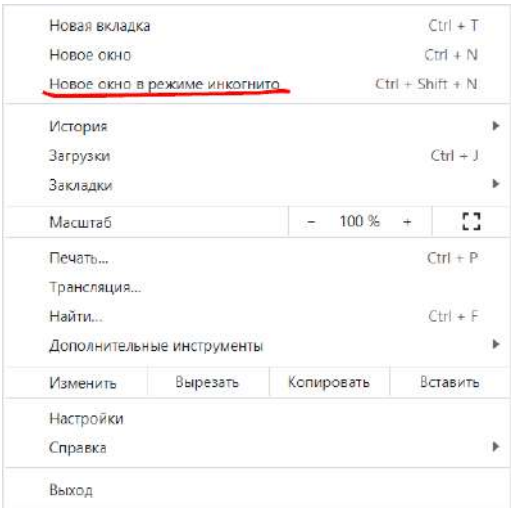

Рис. 6. Включение режима инкогнито

Включить режим инкогнито проще, чем чистить историю посещений и файлы cookie после посещений интернет-ресурсов, но в плане приватности данный режим бесполезен, браузер передает точно такое же количество информации, что и без него. Поэтому идем в настройки и во вкладках «Синхронизация сервисов Google» и «Автозаполнение» отключаем все предоставленные сервисные возможности. Вкладку «Файлы cookie и другие данные сайтов» в разделе «Конфиденциальность и безопасность» настраиваем, как на рис. 7.

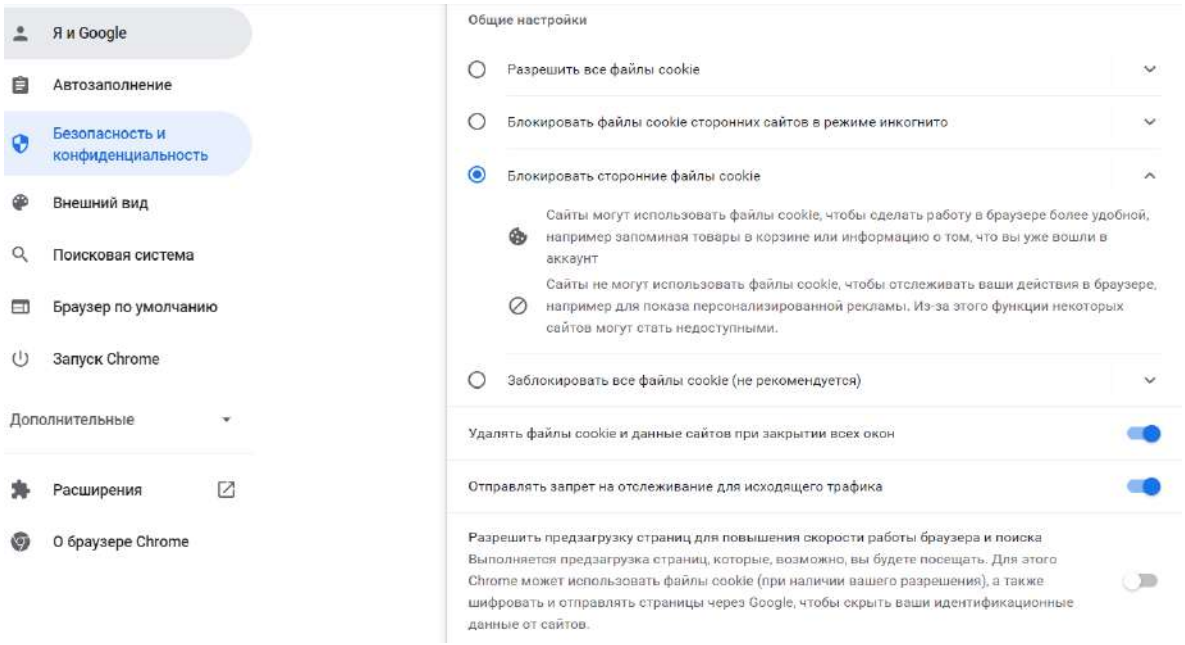

Рис. 7. Настройка Chrome

В результате получаем улучшение состояния приватности, но за счет снижения сервисных возможностей браузера (рис. 8, 9).

Рис. 8. Результат настройки

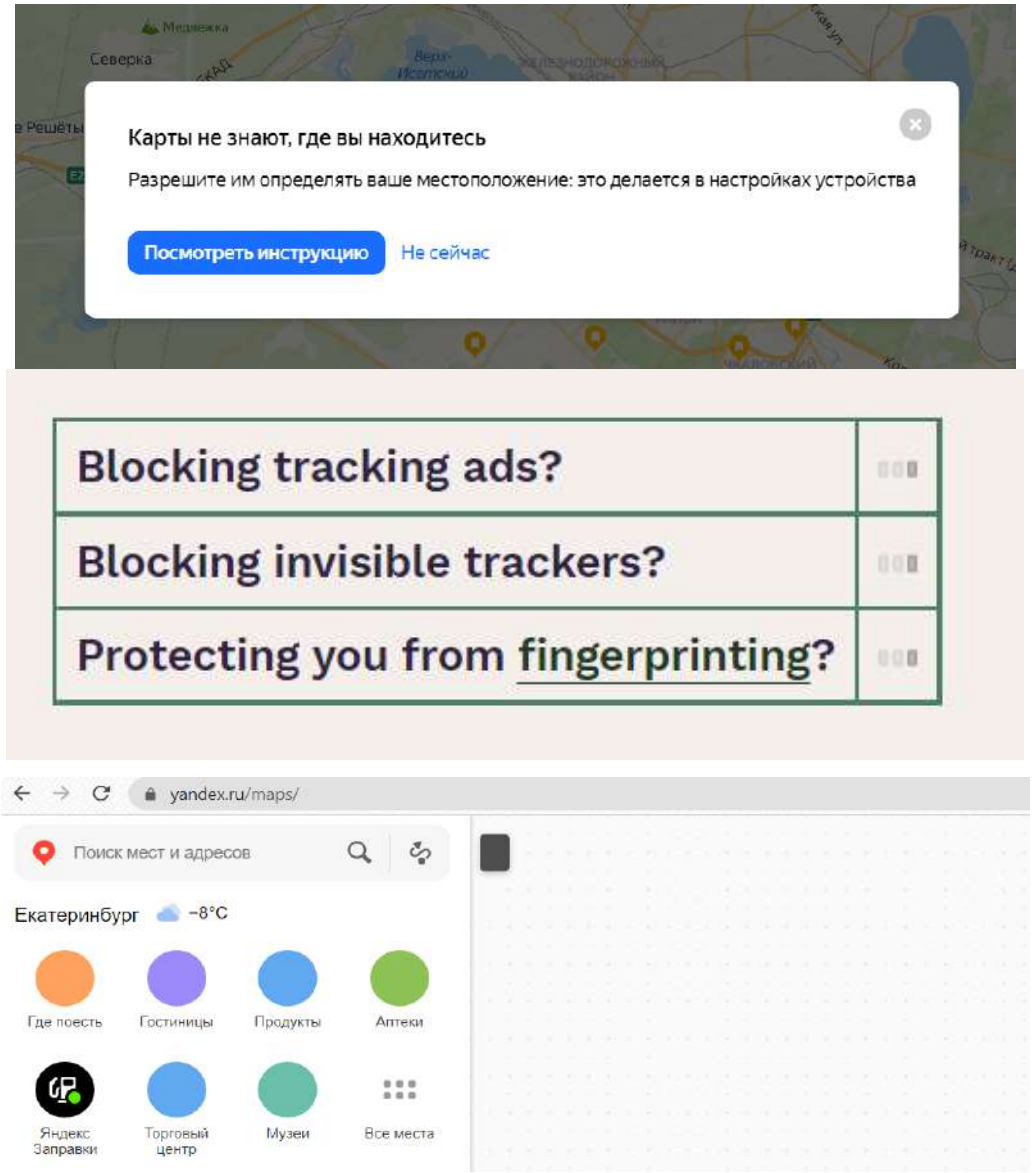

Рис. 9. При полном отключении JavaScript все трекеры перестают работать. Правда, вместе со всем активным содержимым браузера

Другой вариант защиты от трекеров – использование специальных расширений для браузеров. Расширения предназначены для упрощения использования интернета и обеспечивают хороший уровень защиты. Например, расширения uBlock Origin и NoScript являются блокировщиками не только рекламы, но и JavaScript. Они позволяют настраивать процесс блокировки по встроенным фильтрам (рис. 10, 11).

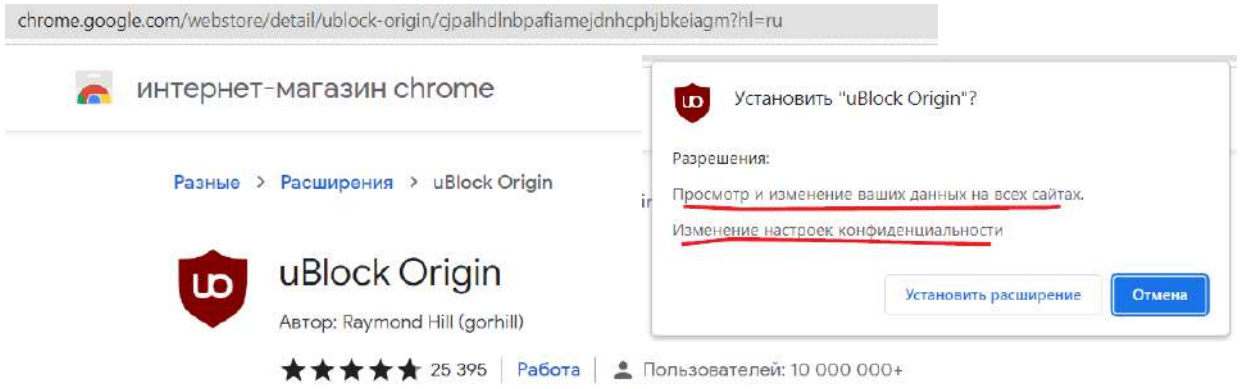

Рис. 10. При установке обратите внимание на запрашиваемые разрешения

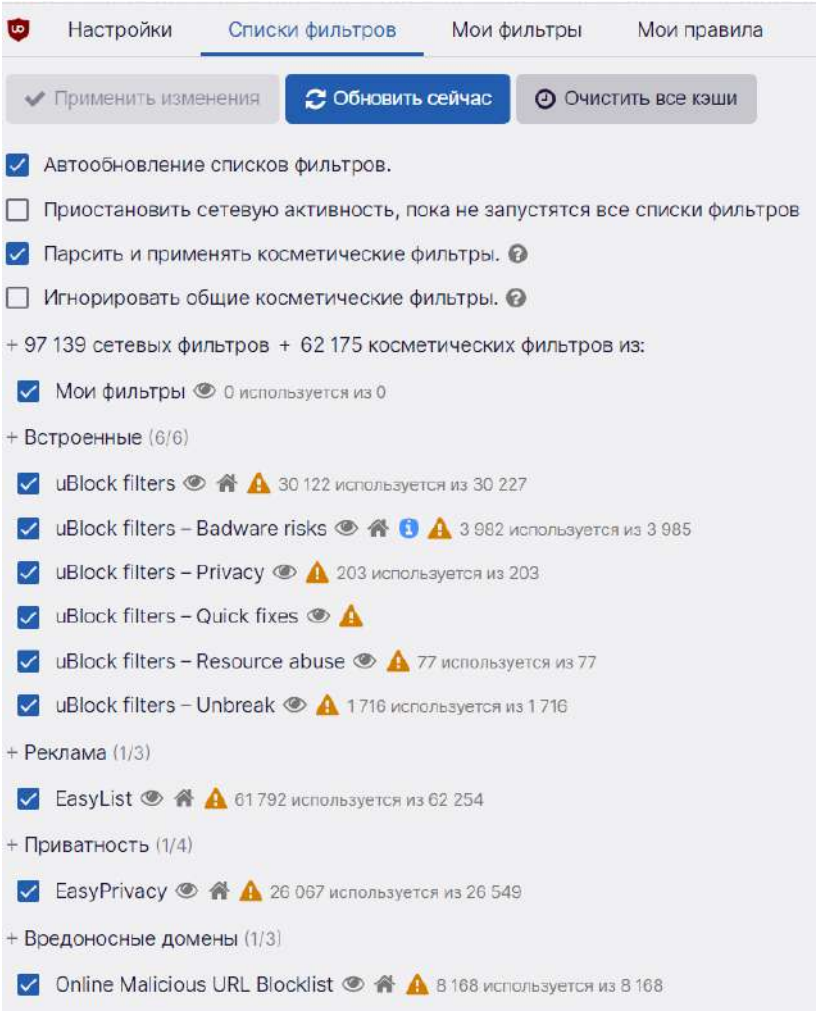

Рис. 11. Настройка фильтров uBlock

Результат проверки представлен на рис. 12.

Рис. 12. Неплохой результат работы uBlock с настройками по умолчанию

Нужно понимать, что нет идеальных средств защиты. Блокировщики делают исключения для компаний, которые обслуживают легитимный контент, необходимый для функционирования сетей доставки контента и видеохостингов. Они ограничивают возможность отслеживания этих доменов, блокируя файлы cookie и доступ к локальному хранилищу, но выделенные трекеры по-прежнему могут получать доступ к IP-адресам, состоянию TLS и некоторым видам данных отпечатков браузеров.

Еще один способ создать проблемы для отслеживающего кода – шифрование DNS-трафика. Система доменных имен (DNS) преобразует удобочитаемые URL, например www.yandex.ru, в IP-адреса, например 5.255.255.80. Когда пользователь вводит доменное имя в адресной строке браузера, тот отправляет запрос на DNS-сервер, который и возвращает IP-адрес для подключения. Запросы и ответы DNS пересылаются по сети в виде обычного текста в незашифрованном виде. Но есть два протокола шифрования DNS: DoH – DNS over HTTPS и DoT – DNS over TLS. В браузеры встроена возможность использования DoH, но по умолчанию она отключена. DoH отправляет DNS-запрос в зашифрованном HTTPS-соединении. Правда, работает DoH только на сайтах, которые могут поддерживать этот протокол. В Mozilla для включения DoH нужно в разделе настроек сети отметить «Включить DNS через HTTPS». Для браузеров на Chromium придется ввести в адресную строку: chrome://flags/#dns-over-https. Принцип работы DoH следующий: пользователь вводит URL сайта в браузере; браузер запрашивает данные DNS-сервера у операционной системы; проверяет, есть ли нужный сервер в списке серверов с поддержкой DoH; и, если да, отправляет зашифрованный DNS-запрос на интерфейс этого сервера; если нет, отправляет обычный DNS-запрос к этому серверу.

Если есть небольшой компьютер, например Raspberry Pi, можно установить фильтр сетевого уровня непосредственно на входе в свою локаль-

ную сеть с помощью Pi-hole. Это специальная сборка на основе Linux, которая позволяет блокировать рекламу и сохранять конфиденциальные данные во время работы в сети. Блокировка происходит на уровне DNS и позволяет гибко настраивать списки запрещенных ресурсов. Он действует как личный DNS-сервер, отклоняя запросы к доменам, которые размещают трекеры. Pi-hole блокирует запросы отслеживания, поступающие от устройств, которые в противном случае трудно настроить, таких как смарт-телевизоры, игровые консоли и устройства интернета вещей. Pi-hole может бороться с рекламными баннерами, скриптами и шпионскими веб-приложениями, которые следят за пользователем. Все это позволяет ускорить загрузку страниц и уменьшить расход трафика.

А как быть с телефонами?

Блокировка трекеров на мобильных устройствах сложнее. Пока не существует единого решения, способного охватить все варианты проникновения трекеров на смартфон. А некоторые виды отслеживания контролировать на определенных устройствах просто невозможно.

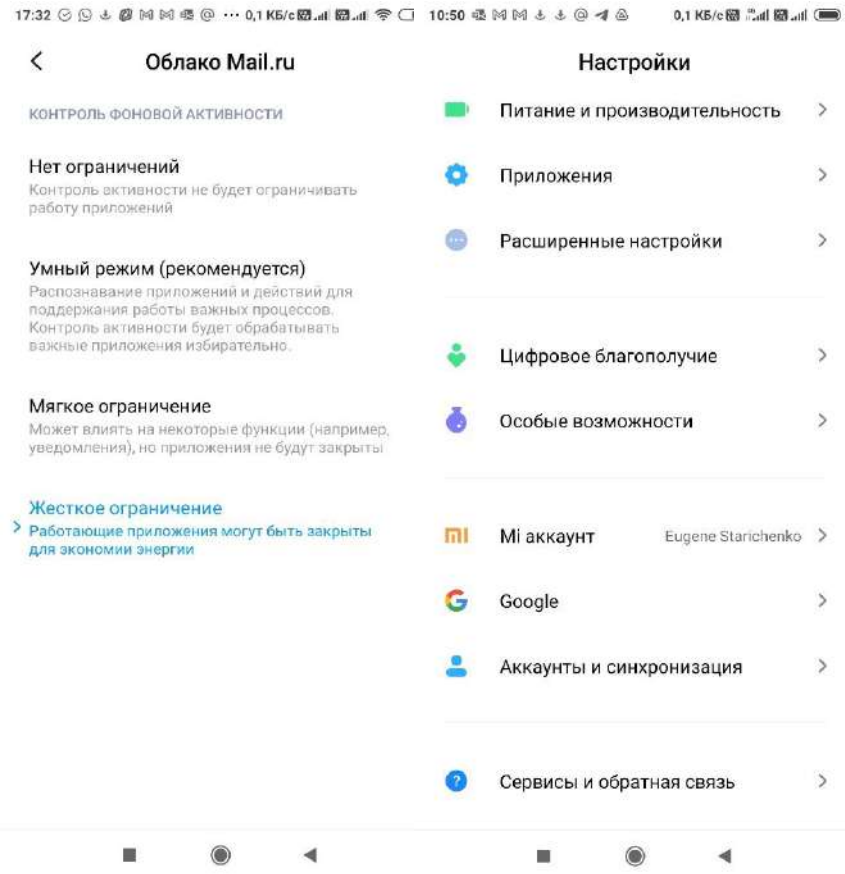

Рис. 13. Установка ограничений на приложения

Первой линией защиты являются настройки устройства. Его операционная система позволяет просматривать и контролировать разрешения, предоставляемые каждому приложению [9]. Необходимо проверить разрешения, которые есть у приложений, и удалить те, которые не нужны. Лучше даже удалить приложения, которые не используются. Есть смысл изменить глобальные параметры сбора и передачи конфиденциальной информации, например местоположения. Для неиспользуемых постоянно приложений надо установить жесткое ограничение фоновой активности для предотвращения пассивного отслеживания.

Мобильные операционные системы также имеют опции для сброса рекламного идентификатора. Рекламный идентификатор – это уникальный идентификатор для рекламы на смартфонах. Он позволяет разработчикам монетизировать свои приложения и услуги. Эти идентификаторы работают так же, как файлы cookie в веб-браузерах, поэтому они отслеживают активность приложений, делятся ими или даже иногда продают их. Таким образом, он используется для предложения рекламы, основанной на ваших интересах. Поскольку идентификатор изменяемый, пользователи могут его сбросить или даже отказаться от персонализированной рекламы. К сожалению, отключить его совсем нельзя, но можно изменить настройки персонализации. Это не избавит вас от рекламы и отслеживания полностью, но затруднит трекерам создание единого профиля о вас.

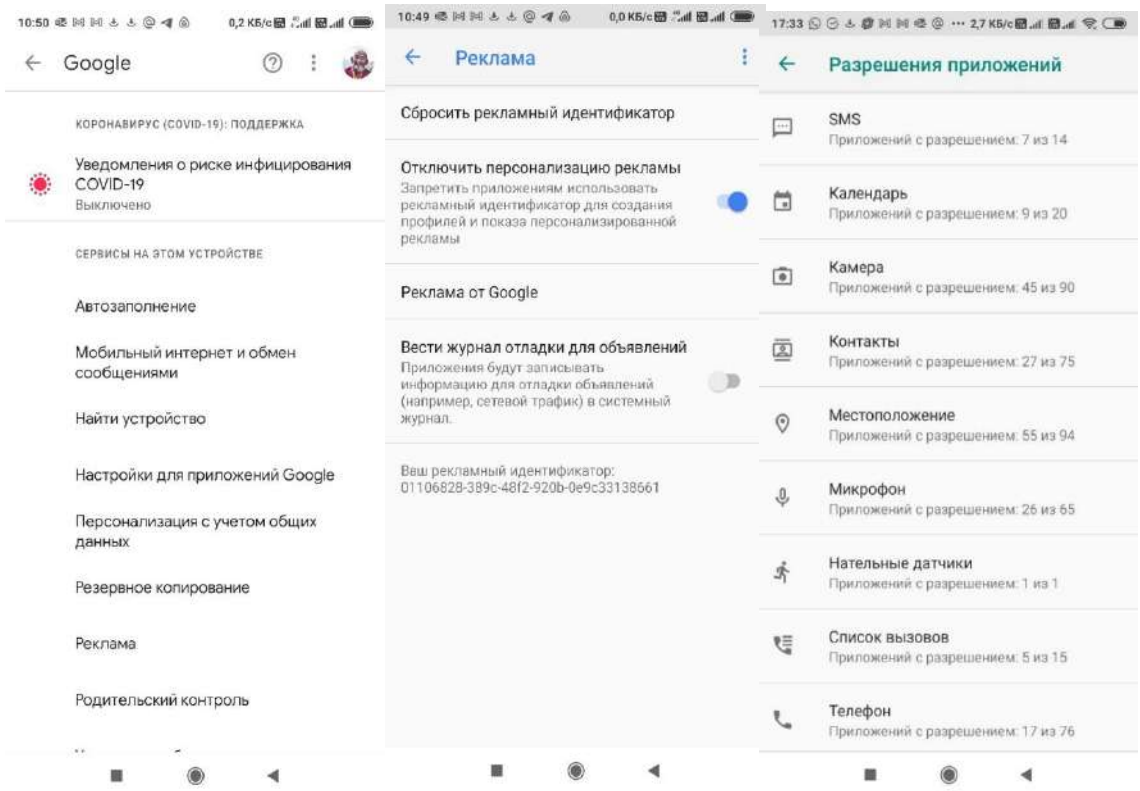

Рис. 14. Сброс персонализации рекламы

Необходимо помнить и о беспроводных сетях, с которыми взаимодействуют смартфоны и планшеты. Они могут собирать идентифицирующую информацию только в том случае, если ваши устройства транслируют свои аппаратные MAC-адреса. Операционные системы рандомизируют их по умолчанию, но электронные книги, смарт-часы и многие другие устройства не имеют такой функции и позволяют использовать их для получения данных о местоположении. Чтобы предотвратить это, лучше держать беспроводные модули связи отключенными, когда вы их не используете. Кроме того, это заметно экономит расход заряда аккумулятора.

Парольная защита

Отслеживание и доступ к персональной информации возможны не только средствами трекеров. Пользователи порой забывают об элементарных средствах защиты своей информации – настройке паролей и антивирусных программ.

Скандалы, связанные с кражей паролей и похищением личных данных, случаются регулярно, только за прошедшие пару лет в сеть утекали пароли пользователей нескольких крупных компаний, популярных почтовых сервисов, хакеры взламывали даже сами сервисы для хранения паролей. Исследования также показали, что одними из главных проблем безопасности онлайн-банков являются авторизация и аутентификация.

Не так давно в сети оказались доступны пароли пользователей нескольких популярных почтовых сервисов (рис. 15).

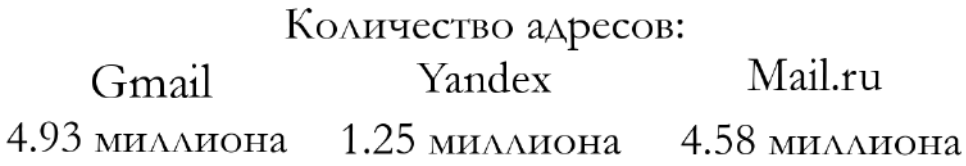

Рис. 15. Результат утечки данных учетных записей почтовых сервисов

Их количество позволило провести статистическое исследование качества пользовательских паролей (рис. 16).

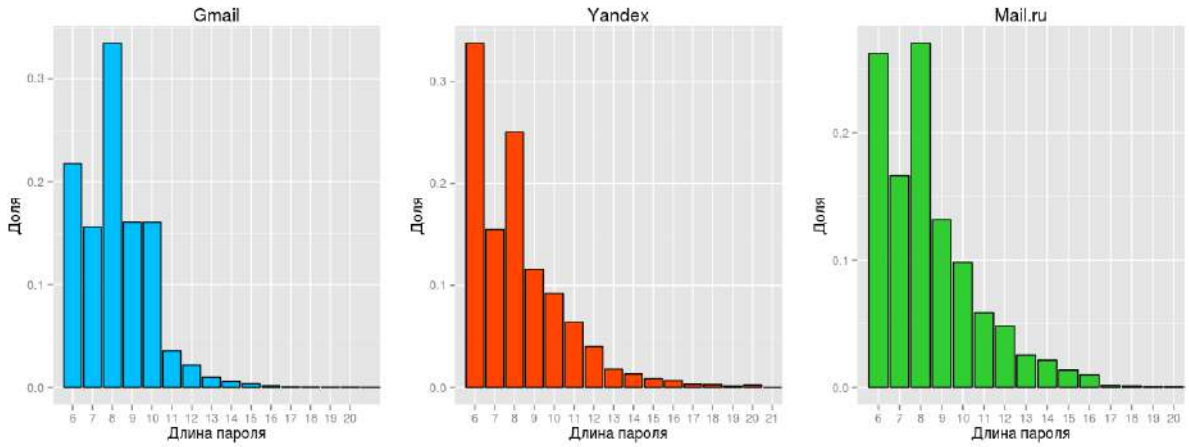

Рис. 16. Распределение длины пользовательских паролей

Надежность пароля оценивается по метрике надежности, основанной на стандарте PCI. За удовлетворение каждого из следующих условий пароль получает условный балл. Пароль содержит:

- не менее семи символов;
- хотя бы одну строчную букву;
- хотя бы одну прописную букву;
- хотя бы одну цифру;
- хотя бы один специальный символ.

Если пароль получает 4 балла из 5, то его считают надежным (очень надежным за 5 из 5), 3 из 5 – средним, 2 из 5 – слабым, 0 или 1 балл – очень слабым. Распределение надежности паролей представлено на рис. 17.

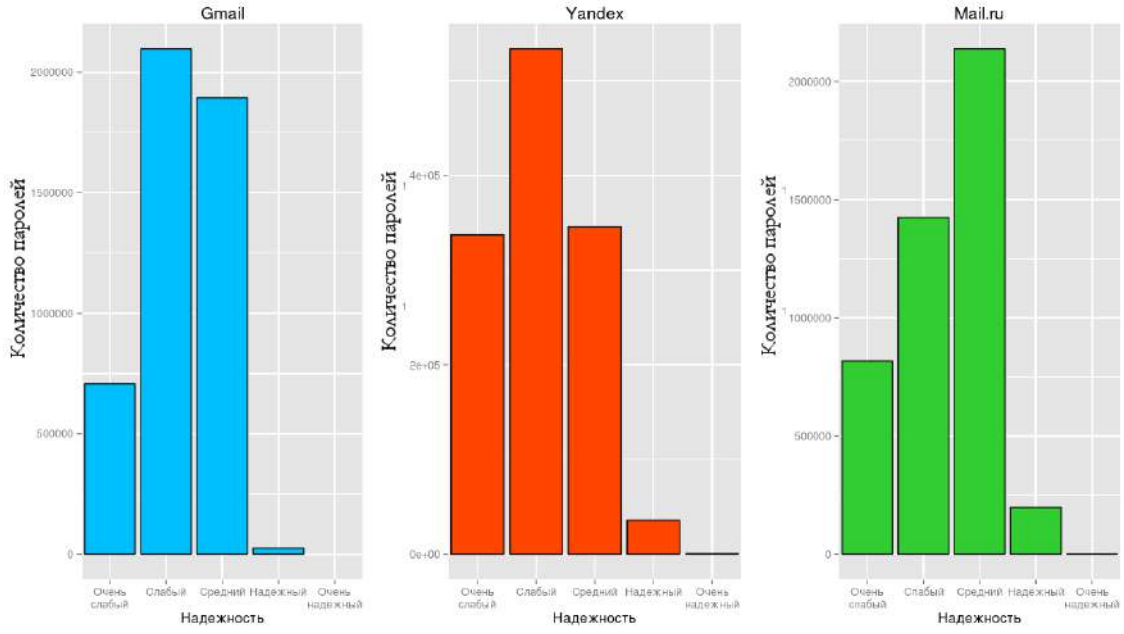

Рис. 17. Распределение надежности паролей

Проверьте, нет ли среди этих паролей ваших (рис. 18):

Gmail	Yandex	Mail.ru
123456	123456	qwerty
password	123456789	123456
123456789	111111	qwertyuiop
qwerty	qwerty	qwe123
12345678	1234567890	qweqwe
111111	1234567	klaster
abc123	7777777	1qaz2wsx
123123	123321	1q2w3e4r
1234567	000000	qazwsx
1234567890	123123	1q2w3e
iloveyou	666666	123qwe

Рис. 18. Топ-20 пользовательских паролей

Существуют онлайн-сервисы, позволяющие проверять пароли на уровень безопасности и создавать безопасные пароли (рис. 19).

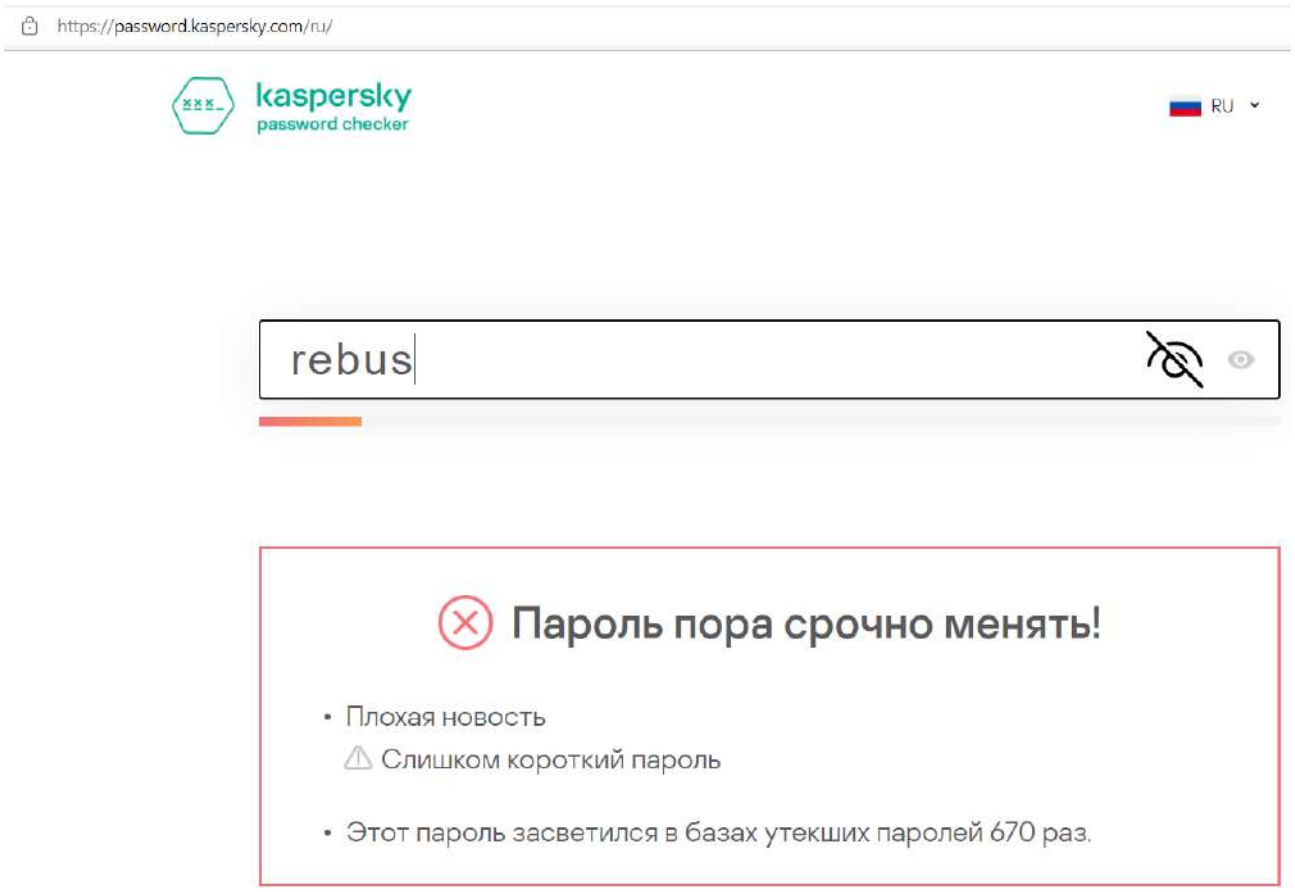

Рис. 19. Сервис проверки паролей от Kaspersky

Антивирусная защита

Одним из важных средств информационной защиты в любой операционной системе, в том числе и в мобильной, являются антивирусные программы. Они давно вышли за пределы только противовирусного функционала и предоставляют комплексную защиту системы от разнообразных угроз. Рассмотрим работу с подобным комплексом безопасности на примере Kaspersky Endpoint Security.

Начиная работу с установленной системой, нужно убедиться в актуальности антивирусных баз, обновить их при необходимости, а также настроить параметры обновления.

Чтобы обновлять модули программы, а не только антивирусные базы, включите опцию «Обновлять модули программы». Это устраняет уязвимости программы, добавляет новые функции или улучшает существующие (рис. 20). Обновления можно сохранять в локальную папку на случай переустановки системы или предоставления возможности обновления для других компьютеров в сети (например, в домашней).

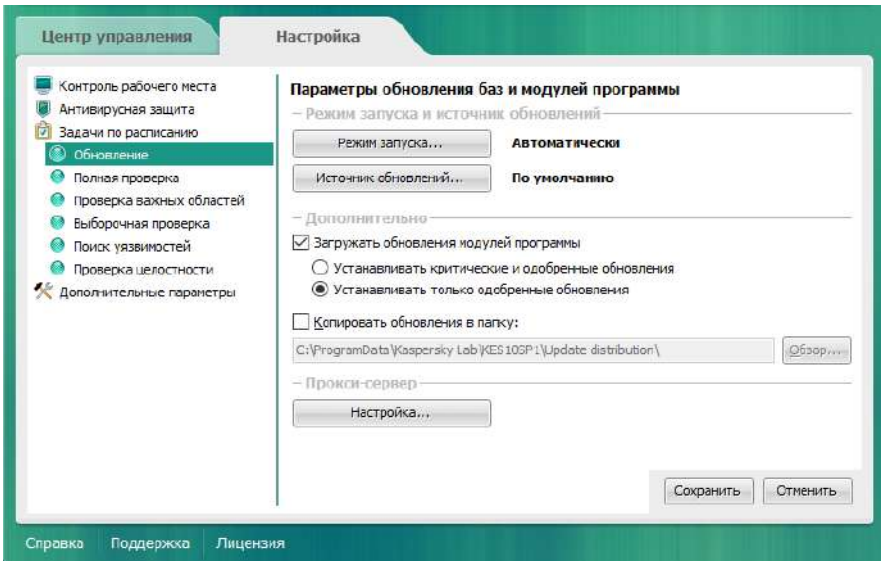

Рис. 20. Настройка параметров обновления антивирусных баз

Можно настроить автоматический, ручной запуск или запуск обновления по расписанию, а также отложить запуск задачи после старта программы.

Автоматически. В этом случае программа запускает задачу обновления в зависимости от наличия пакета обновлений в источнике обновления.

- Вручную – для запуска задачи обновления вручную.
- По расписанию – для настройки расписания запуска задачи обновления.

В качестве источника обновлений можно указать:

- серверы Лаборатории Касперского;
- FTP-сервер;
- HTTP-сервер;
- папку общего доступа.

Если в качестве источников обновлений выбрано несколько ресурсов, в процессе обновления программа обращается к ним по списку и выполняет задачу, используя пакет обновлений первого доступного источника.

Опция «Региональные параметры» позволяет задать расположение ближайшего сервера обновлений Лаборатории Касперского, что поможет сократить время получения обновлений. По умолчанию в параметрах обновления используется информация о текущем регионе из реестра операционной системы.

Текущее состояние антивирусных баз можно видеть на закладке «Центр управления» при открытом блоке «Управление задачами».

Для принудительного запуска задачи обновления антивирусных баз пройдите последовательность: Центр управления – Управление задачами – Обновление – Запустить обновление (рис. 21).

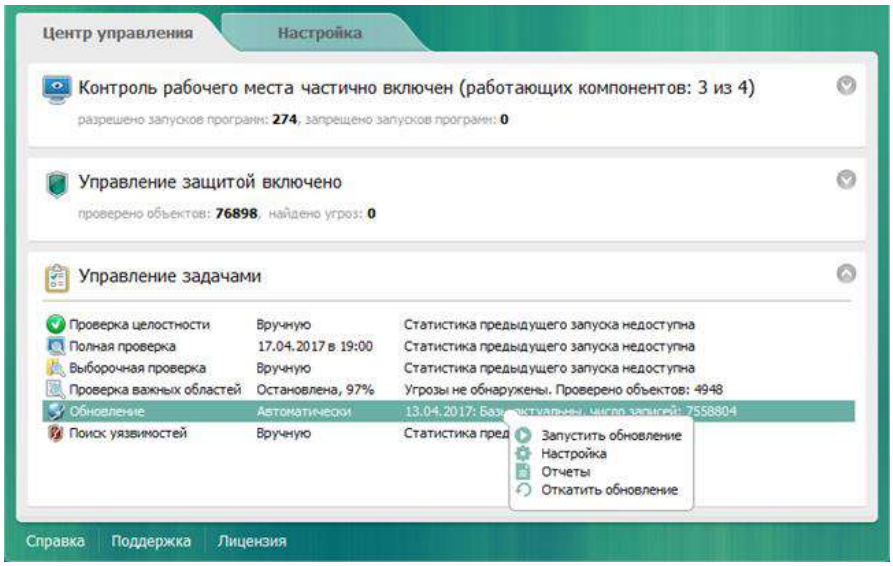

Рис. 21. Запуск обновления антивирусных баз

Kaspersky при каждом выполнении задачи обновления создает резервную копию используемых баз и модулей программы, что позволяет вернуться к ним в случаях, если:

- новая версия антивирусных баз содержит некорректную сигнатуру, из-за которой блокируется безопасная программа;
- в процессе обновления антивирусные базы были повреждены.

Откат к предыдущим базам можно выполнить только на одно обновление назад. Чтобы откатить последнее обновление, пройдите последовательность: Центр управления – Управление задачами – Обновление – Откатить обновление.

Для обеспечения постоянной защиты в режиме реального времени в современных антивирусных программах есть модуль мониторинга системы. Он использует следующие технологии:

- Защита от эксплойтов. Блокирует вредоносные программы, которые используют уязвимости в программном обеспечении. Включает в себя:
  - контроль запуска исполняемых файлов из уязвимых программ и браузеров;
  - контроль подозрительных действий уязвимых программ (например, повышение прав выполняемой уязвимой программы, запись в память системы других процессов);
  - мониторинг действий программ предыдущих запусков (например, была ли запущена программа пользователем или эксплойтом);
  - отслеживание источника вредоносного кода (например, удаленный веб-адрес или браузер, который запустил скачивание зараженного файла);
  - предотвращение использования уязвимостей в программах.
- Контроль активности программ. При обнаружении программы с подозрительной активностью выполняет действие, указанное в настройках.
- Откат действий вредоносной программы. Информация о подозрительных действиях в системе собирается не только в рамках текущей сессии работы, но и за время предыдущих сессий. Это позволяет выполнить отмену всех совершенных программой действий, если программа будет признана вредоносной.
- Защита от программ-крипторов. Крипторы – это вирусы, которые шифруют данные и требуют выкуп за возврат файлов в исходное состояние. Если программа-криптор пытается зашифровать файл, антивирус автоматически создает резервную копию данных. Если файл будет зашифрован, антивирус восстановит его из резервной копии.

Для включения мониторинга пройдите последовательность Настройка – Антивирусная защита – Мониторинг системы и отметьте соответствующий чекбокс (рис. 22).

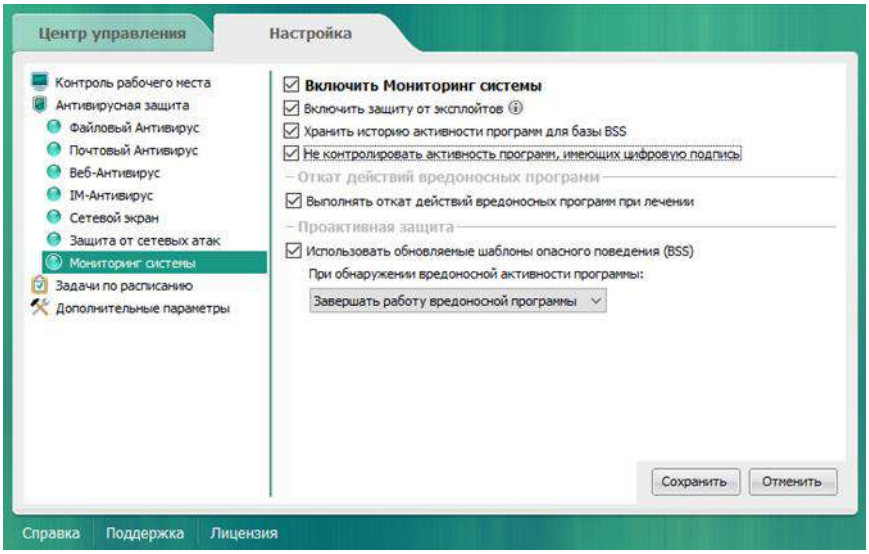

Рис. 22. Настройка режима мониторинга

Самозащита – это компонент, который обеспечивает защиту антивирусной системы от вредоносных программ, пытающихся заблокировать ее или удалить с компьютера.

Самозащита позволяет предотвратить:

- изменение/удаление собственных файлов, включая файлы программы, антивирусные базы, файлы карантина, трассировки;
- изменение/удаление ключей из системного реестра;
- завершение процессов программы.

Для включения/отключения самозащиты пройдите последовательность Настройка – Дополнительные параметры и отметьте соответствующий чекбокс.

Для уменьшения вероятности шифрования данных вредоносными программами-вымогателями следует держать включенными следующие компоненты защиты:

- Мониторинг системы и BSS. Мониторинг системы анализирует активность программ, а BSS – их поведение.
- Контроль активности программ. Компонент повышает уровень анализа подозрительных файлов и увеличивает вероятность обнаружения вредоносных программ.
- Kaspersky Security Network.

Убедитесь, что включены «Мониторинг системы» и хранение истории активности. Включение: Настройка – Антивирусная защита – Мониторинг системы.

Для настройки контроля активности программ пройдите последовательность: Настройка – Контроль рабочего места – Контроль активности программ – Ресурсы (рис. 23).

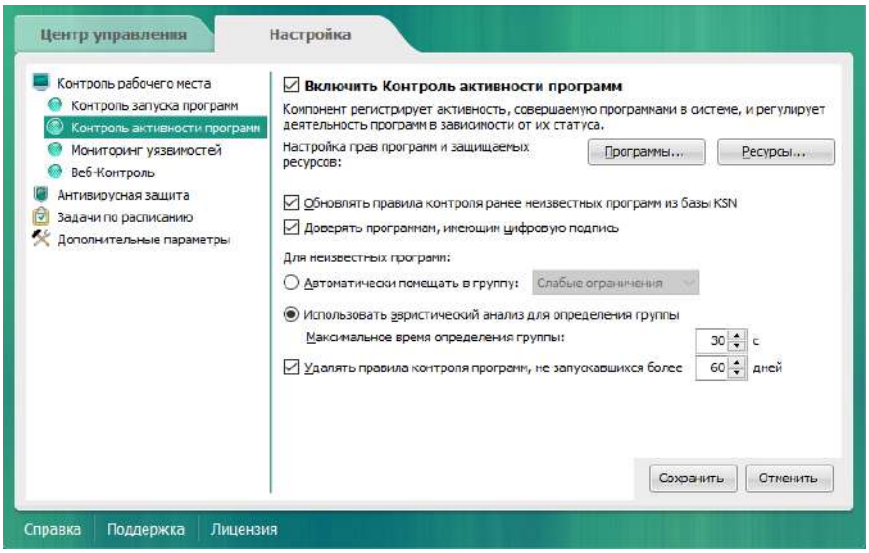

Рис. 23. Настройка контроля активности программ

Для узла «Персональные данные» добавьте категорию «Файлы под защитой», а в нее несколько подкатегорий (например, «Документы», «Фотки» и т. п.). В каждую категорию добавьте защищаемые каталоги (рис. 24).

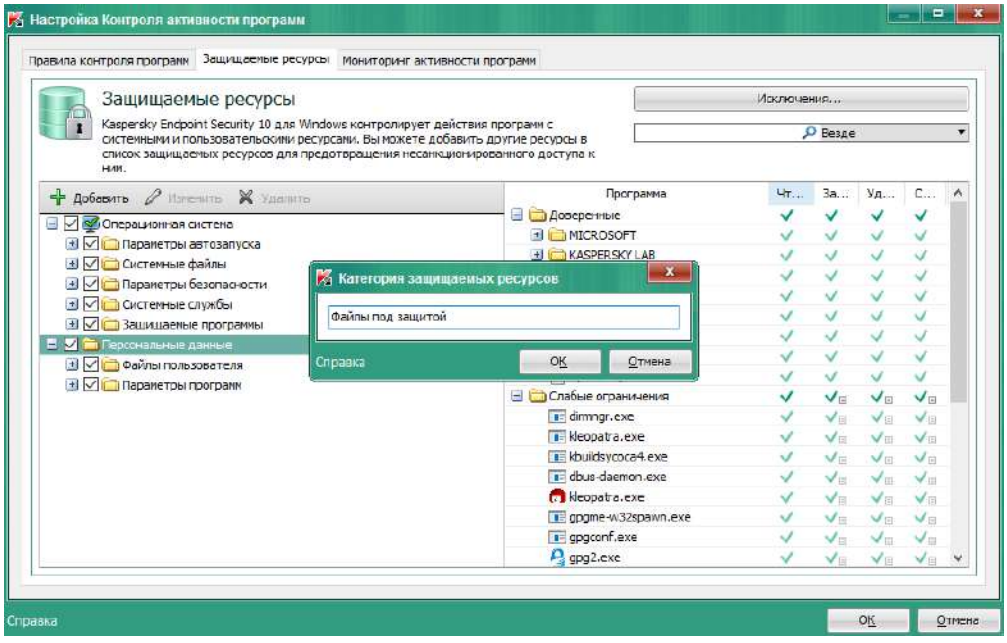

Рис. 24. Защита персональных данных

Настройте права доступа для категории «Файлы под защитой», выставив запрет на запись, удаление и создание. Убедитесь, что необходимые для работы программы находятся в доверенной группе (рис. 25).

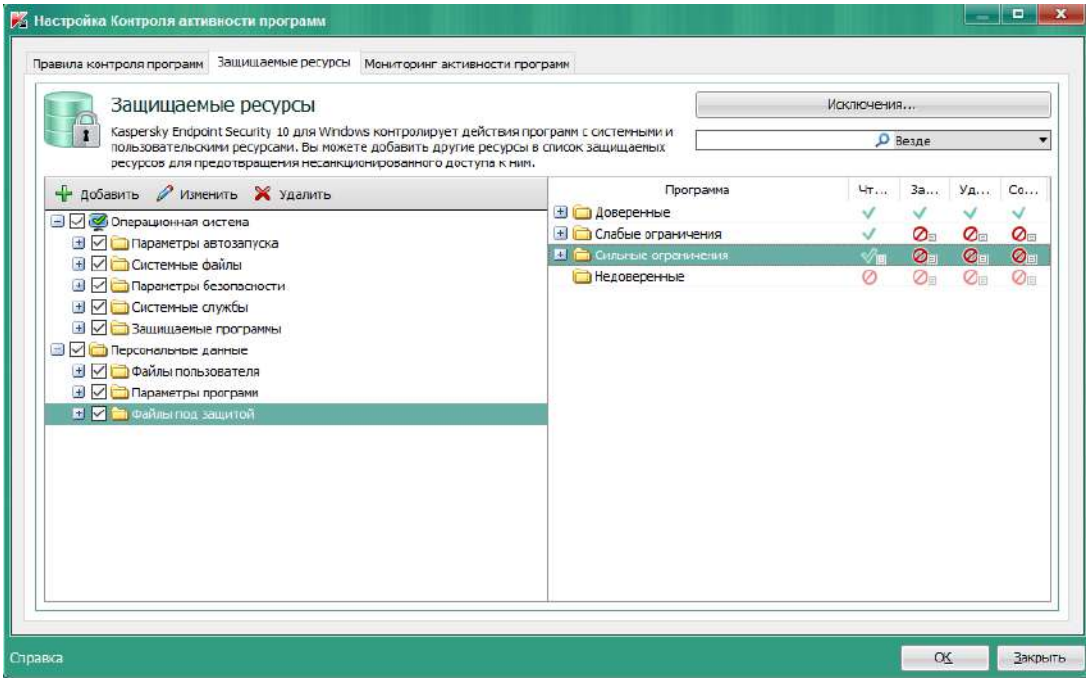

Рис. 25. Установление ограничений

Заключение

По данным компании InfoWatch, с января по сентябрь 2020 года в России утекло 96,5 млн записей персональных данных и платежной информации. При этом доля утечек, связанных с мошенническими действиями, превышает 10 %; в мире этот показатель втрое ниже [12]. Персональные данные являются предметом продажи и имеют совершенно конкретную стоимость. Например, базы данных по всем регионам России, содержащие Ф. И. О., пол, телефон, полные паспортные данные, СНИЛС, адрес регистрации и проживания, стоят 20–25 копеек за одну запись. Такие базы используются в основном для спама и мелкого мошенничества. Фотография паспорта и фотография владельца паспорта с паспортом в руках – от 150 рублей за комплект; комплект из сканов паспорта, СНИЛС, водительского удостоверения и ИНН – от 300 рублей; дебетовые карты российских банков – от 5 000 до 12 000 рублей за карту [4].

Защититься от мошенников, использующих современные технические и программные средства, практически невозможно. Единственное средство – не использовать электронные устройства, не выходить в интернет, уехать (а лучше уйти) в далекую деревню, где пока нет камер наблюдения, и расплачиваться наличными. Естественно, это слишком радикальные меры в современном мире, поэтому мы можем хотя бы усложнить работу трекеров и мошенников, собирающих информацию о нас. Если данные сложно получить, возрастает стоимость, и связываться с их получением становится экономически невыгодно.

Библиографический список

1. Dan, York. IPv6 Privacy Addresses Provide Protection Against Surveillance And Tracking / York Dan. – Текст : электронный // www.internetsociety.org [сайт]. – URL: https://www.internetsociety.org/blog/2014/12/ipv6-privacy-addresses-provide-protection-against-surveillance-and-tracking/ (дата обращения: 21.03.2022).
2. How Long Does an IP Address Stay Attached to a Home or Business? – Текст : электронный // eltoro.com [сайт]. – URL: https://eltoro.com/how-long-does-an-ip-address-stay-attached-to-a-home-or-business/ (дата обращения: 21.03.2022).
3. Signals from the Crowd: Uncovering Social Relationships through Smartphone Probes. – Текст : электронный // http://conferences.sigcomm.org [сайт]. – URL: http://conferences.sigcomm.org/ imc/2013/papers/imc148-barberaSP106.pdf (дата обращения: 21.03.2022).
4. Анализ цен черного рынка на персональные данные и пробив. – Текст : электронный // habr.com [сайт]. – URL: https://habr.com/ru/company/devicelockdlp/blog/430914/ (дата обращения: 21.03.2022).
5. Брокеры данных: кто, где и как продает информацию о нас. – Текст: электронный // rb.ru [сайт]. – URL: https://rb.ru/story/data-brokers/ (дата обращения: 21.03.2022).
6. Григорьев, А. Протокол IPv6: что это такое и как он работает / А. Григорьев. – Текст : электронный // timeweb.com [сайт]. – URL: https://timeweb.com/ru/community/articles/protokol-ipv6-chto-eto-takoe-i-kak-on-rabotaet (дата обращения: 21.03.2022).
7. Защитите личные данные в интернете. – Текст : электронный // privacy.kaspersky.com [сайт]. – URL: https://privacy.kaspersky.com/ (дата обращения: 21.03.2022).
8. Как веб-сайты тайно записывают вашу деятельность с помощью сценариев воспроизведения сеанса. – Текст : электронный // helpexe.ru [сайт]. – URL: http://helpexe.ru/bezopasnost/kak-veb-sajty-tajno-zapisyvajut-vashu-dejatelnost (дата обращения: 21.03.2022).
9. Как настраивать разрешения для приложений на телефоне Android. – Текст : электронный // support.google.com [сайт]. – URL: https://support.google.com/android/answer/9431959?hl=ru (дата обращения: 21.03.2022).
10. Как рекламщики узнают, какие приложения вы используете. – Текст : электронный // www.kaspersky.ru [сайт]. – URL: https://www.kaspersky.ru/blog/android-device-identifiers/25870/ (дата обращения: 21.03.2022).
11. Конов, С. Избавляемся от отслеживания и сбора данных в браузерах / С. Конов. – Текст : электронный // www.anti-malware.ru [сайт]. – URL: https://www.anti-malware.ru/practice/methods/Get-rid-of-tracking-in-browsers (дата обращения: 21.03.2022).
12. Побочное явление цифровизации: как в России крадут и продают персональные данные – Текст : электронный // www.forbes.ru [сайт]. – URL: https://www.forbes.ru/tehnologii/433651-pobochnoe-yavlenie-cifrovizacii-kak-v-rossii-kradut-i-prodayut-personalnye-dannye (дата обращения: 21.03.2022).
13. Продажа и покупка персональных данных – Текст : электронный // goodlucker.ru [сайт]. – URL: https://goodlucker.ru/zakon/personal-information.html (дата обращения: 21.03.2022).
14. Распознавание автомобильных номеров. – Текст : электронный // securityrussia.com [сайт]. – URL: https://securityrussia.com/blog/avto-nomera.html (дата обращения: 21.03.2022).

15. Слежка с помощью браузера. – Текст : электронный // zen.yandex.ru : [сайт]. – URL: https://zen.yandex.ru/media/irozysk/slejka-s-pomosciu-brauzera-5b20080dd0745b00a92a78d3 (дата обращения: 21.03.2022).
16. developer.android.com [сайт]. – URL: https://developer.android.com/reference/android/Manifest.permission#READ_PHONE_STATE (дата обращения: 21.03.2022).
17. developer.mozilla.org [сайт]. – URL: https://developer.mozilla.org/en-US/docs/Web/HTTP/Methods/POST (дата обращения: 21.03.2022).
18. doma35.ru [сайт]. – URL: https://doma35.ru/computers/kuki-fayly-gde-hranyatsya-na-kompyutere/ (дата обращения: 21.03.2022).
19. github.com [сайт]. – URL: https://github.com/pi-hole/pi-hole (дата обращения: 21.03.2022).
20. www.tutorialspoint.com [сайт]. – URL: https://www.tutorialspoint.com/how-to-obtain-the-phone-number-of-the-ios-phone-programmatically (дата обращения: 21.03.2022).
21. Тысячи приложений нарушают правила Google Play и шпионят за детьми. – Текст : электронный // www.iguides.ru [сайт]. – URL: https://www.iguides.ru/main/security/tysyachi_prilozheniy_narushayut_pravila_google_play_i_shpionyat_za_detmi/ (дата обращения: 21.03.2022).
22. Уникальная идентификация Android-устройства. – Текст : электронный // russianblogs.com [сайт]. – URL: https://russianblogs.com/article/10291353405/ (дата обращения: 21.03.2022).
23. Хлипко, Е. Как я собирала Mac-адреса и почему старгетировать по ним рекламу оказалось не так просто / Е. Хлипко. – Текст : электронный // vc.ru [сайт]. – URL: https://vc.ru/marketing/127713-kak-ya-sobirala-mac-adresa-i-pochemu-stargetirovat-po-nim-reklamu-okazalos-ne-tak-prosto (дата обращения: 21.03.2022).
24. Что такое рекламный идентификатор на Android? Как сбросить его, чтобы ограничить рекламу на вашем телефоне. – Текст : электронный // websetnet.net [сайт]. – URL: https://websetnet.net/ru/what-is-advertising-id-on-android-how-to-reset-it-to-limit-ads-on-your-phone/ (дата обращения: 21.03.2022).