УДК 004.62

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ПОЛЬЗОВАТЕЛЕЙ СЕГМЕНТА РУНЕТ

Киренберг А.Г., доцент кафедры ИБ
Евдокимов И.В., студент гр. ИБс-211, 2 курс
Безденежных И.В., студент гр. ИБс-211, 2 курс
Кузбасский государственный технический университет
имени Т.Ф. Горбачева,
г. Кемерово

Аннотация: Информационная безопасность должна быть обеспечена не только для информационных систем, но и для человека, его личного цифрового пространства. Нарушения информационной безопасности человека проявляется не только в виде взломов его личных страниц в социальных сетях или несанкционированный доступ к его компьютеру или гаджету, но и в виде психологического воздействия на его ментальность. Такие воздействия могут негативно влиять на поведение человека, в результате чего есть опасность принятия неверных решений, способных нанести ему как морально-психологическую травму, так и финансовый или даже физический ущерб. в т.ч. и с риском для жизни. Научная новизна статьи состоит в определении нескольких подходов в борьбе с мошенническими сайтами, а также с сайтами распространения фейковой информации.

Ключевые слова: информационная безопасность частных пользователей, фейковая информация, сегмент Рунет, подходы к повышению информационной безопасности.

Интернет как явление, информационное пространство, а также как хранилище разнообразной мировой информации уже давно и прочно вошел в обиход, и мы уже не представляем свою жизнь без него. Безусловно, в Интернете много полезной информации самого разного профиля, но в тоже время много и бесполезной, а нередко даже и опасной. Это обусловлено тем, что сеть Интернет не имеет единого центра управления или собственника, а значит никто не обеспечивает фильтрацию контента на уровне доменов (сайтов). Любое желающее физическое или юридическое лицо может создать свой сайт и наполнить его чем угодно, зная, что цензура отсутствует. Разновидностей типов сайтов очень много, но в данной статье мы заострим внимание лишь на двух типах – ***новостные сайты*** (к которым отчасти относятся и поисковые системы) и ***одностраничные сайты продаж***, поскольку именно эти типы сайтов наиболее причастны к проблематике информационной и финансовой безопасности частных пользователей сегмента Рунет, а также к вопросам информационной гигиены.

Сразу необходимо пояснить: в данной статье к нарушению ИБ частного пользователя авторы относят в т.ч. и распространение недостоверных (фейковых) сведений, оказывающих на него психологическое воздействие, а также утечку его персональных данных или финансовых средств обманным путем. В настоящее время наиболее известны 5 основных каналов распространения фейковых новостей через Интернет – рис. 1

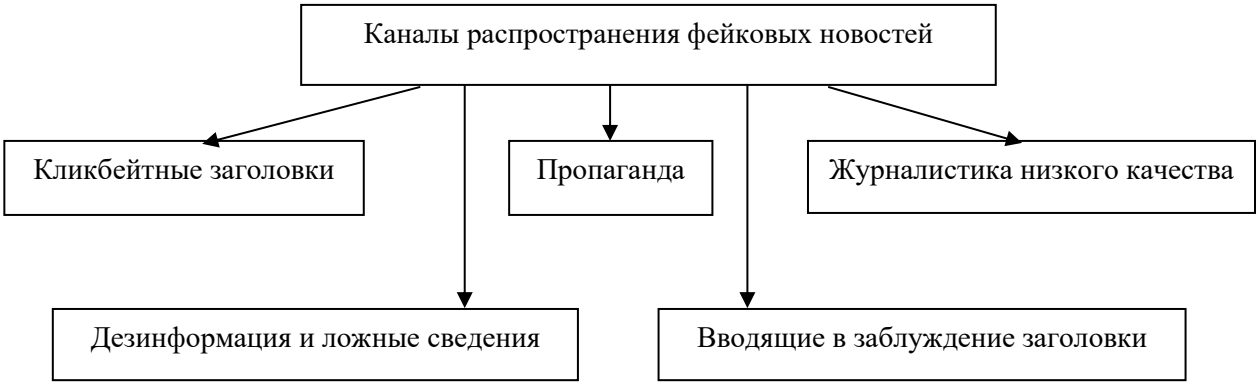

Рис 1 – Существующие каналы распространения фейковых новостей

Поясним данную схему.

1***) Кликбейтные*** заголовки. Создаются с целью привлечения внимания и увеличения количества кликов на сайт или страницу. Они могут быть привлекательными и интересными, но не всегда соответствуют содержанию статьи или новости.

2) ***Пропаганда***. Распространение информации, которая нацелена на убеждение людей в определенной идее или установке. Пропаганда может быть использована для манипуляции общественным мнением и формирования определенных убеждений.

3) ***Журналистика низкого качества***. Проявляется в создании новости или статьи, которая содержат ошибки, неточности или не подтвержденные факты. Они могут быть написаны без должной проверки и исследования, что может привести к распространению ложной информации.

4) ***Вводящие в заблуждение заголовки***. Они создают ложное впечатление о содержании статьи или новости. Они так же могут быть использованы для привлечения внимания и увеличения посетителей сайта, но не всегда соответствуют действительности.

5) ***Дезинформация и Ложные сведения***. Распространяется такая информация с целью воздействия на массовое сознание и формирования определенных убеждений. Они могут быть использованы для манипуляции общественным мнением, создания политической нестабильности или дискредитации оппонентов.

Рассмотрим особенности сайтов первого типа – новостных сайтов.

Некоторые новостные сайты могут использовать сенсационные заголовки, чтобы привлечь внимание читателей и увеличить количество просмотров.

Однако, зачастую эти заголовки не соответствуют содержанию статьи, что может привести к неверному пониманию и искажению фактов.

Практически каждый из нас как минимум хотя бы 1 раз в день с экрана компьютера или смартфона становится читателем новостных дайджестов, отображаемых на главных страницах поисковых систем: yandex / dzen, mail, rambler, а также многих других известных сайтах.

Источники, которые предоставляют нам эти дайджесты и более подробную информацию при клике на них разделяются на 3 основные группы: [1]

1. Агрегаторы первого эшелона, которые по совместительству являются и поисковыми системами, указанными выше и их всего 3. Часть фреймов сайтов агрегаторов отдается под размещение новостных блоков, полученных от информационных агентств, а другая часть предназначена для сугубо коммерческого использования любым желающего разместить на этой площадке свою рекламу.

2. Информационные агентства – их всего 5, в т.ч. 3 наиболее известных всем: РИА-новости, ТАСС, Интерфакс;

3. Интернет-издания, которых насчитывается более 100, представляющие собой сайты некоторых телевизионных каналов, которые вещают в т.ч. и новостные блоки, а также сайты газет или журналов федерального и регионального уровней. На наш взгляд, эта группа сайтов источников является наиболее слабо контролируемой и на ней следует остановится подробнее.

В Рунете к этой группе сайтов относятся как достаточно известные, например: интернет-газета Lenta.ru, электронная газета «Утро.ру» и многие другие [2], а также издания, которые известны нам под термином «желтая пресса», в которой владельцы этих сайтов предоставляют все желающим на коммерческой основе услуги по формированию определенного настроения в народных массах, манипулирования сознанием путем размещения на своих страницах непроверенной, сомнительной, искаженной, устаревшей или откровенно ложной информации или фейков от различных источников [3].

Некоторые такие сайты с подобным контентом агрессивно отображаются в верхних позициях домашних страниц мобильных веб-браузеров. Так, например, сайт akket.com, имеющий негативную популярность у многих пользователей Рунета из-за того, что заголовки многих статей не соответствуют самой сути текста или вырваны из контекста других статей. Например, заголовок «Во всех банкоматах. «Сбербанк» установил комиссию за снятие наличных с банковских карт» присвоен статье, в которой говорится о том, что Сбербанк действительно берет комиссию 1%, но только при снятии наличных в чужих банкоматах, а не в любом случае, как можно было бы предположить из заголовка статьи.

Причем переход на «желтые ресурсы» может осуществляться даже с вполне известных и надежных сайтов, для этого достаточно сделать 1-2 перехода с домашней страницы своего веб-браузера, с которой начинается веб-сёрфинг. Также было замечено, что содержимое страниц некоторых ресурсов может отличаться для десктопной и мобильной версии браузеров. Например,

некий приморский региональный ресурс primpress.ru при присмотре с компьютера содержит вполне обычный достоверный информационно-новостной контент, однако если мы откроем данный сайт с домашней страницы мобильного браузера, то прокрутив немного вниз мы увидим раздел «Новости партнеров», в котором кликнув по любой ссылке этого раздела попадаем на одного из таких партнеров, которыми являются сайты-агрегаторы новостей второго или даже третьего эшелона, причем преимущественно фейковых. Найти данную информацию можно и с декстопной версии браузера вручную, однако путь в этом случае будет несколько длиннее. Часто для маскировки фейковая информация может чередоваться с блоками достоверной информации.

Какой вред наносят сайты фейковых новостей? На первый взгляд, казалось бы, вреда немного – они не разводят людей на деньги, не унижают достоинство человека, но это только лишь «вершина айсберга». На самом деле при грамотном искажении или подборе контента эти сайты оказывают влияние не общественное сознание людей, а если количество таких подверженных влиянию будет достаточно велико, то последствия такого воздействия могут быть весьма ощутимыми даже на уровне целого государства. Например, если на таких ресурсах запустить фейк о том, что с завтрашнего дня Сбербанк прекратит выдачу наличных или заморозит счета вкладчиков на неопределенный период, то с большой долей вероятности на следующий день мы увидим огромные очереди в отделениях банка и банкоматах с целью снять свои средства и тем самым банковской системе будет нанесен серьезный урон. Подобный принцип можно применить не только к банковской сфере, но и к аптечной, торговым сетям, АЗС и т.п… Создание искусственного ажиотажа или нагнетание нездоровой политической обстановки в государстве, которая может перерасти даже в гражданскую войну или принудительной смене власти – одни из основных задач подобных сайтов.

Теперь рассмотрим особенности сайтов второго типа – одностраничных сайтов по продаже чего-либо (другое название – «лендинговые» или «посадочные» страницы). Одностраничные сайты продаж товаров могут использовать манипулятивные методы воздействия на потенциального покупателя, такие как ограниченное предложение или скидки, чтобы заставить пользователей совершить покупку в спешке. Кроме того, они могут использовать фотографии и описания товаров, которые не соответствуют действительности, тем самым обманывая покупателя.

Такие сайты создаются очень легко и быстро, а значит затраты на их создание (в отличии от полноценных интернет-магазинов) минимальны. Попасть на такие страницы можно чаще всего с новостных сайтов второго и третьего эшелонов, сайтов, относящихся к категории «желтой прессы», хотя иногда это может быть доступно даже из известных топовых новостных сайтов, агрегаторов, поисковиков, сайтов соцсетей.

Дело в том, что зачастую нижняя часть страницы многих известных сайтов сдается для рекламных целей в аренду и причем стоимость нижних фреймов существенно ниже, чем в верхней или центральной части сайтов по при-

чине того, что не все пользователи могут прокрутить страницу вниз до конца, а значит вероятность клика по ссылкам нижней зоны меньше. Таким образом, если на популярных известных сайтах контент верхней и средней частей сайта еще хоть как-то проверяется перед размещением, то внизу страницы за небольшие деньги можно разместить почти все что угодно, и такой подход является выгодным как для арендодателя пространства сайта (ведь от лишних денег не хочет отказываться никакой сайт вне зависимости от своего статуса и репутации), так и для арендатора. Именно во фреймах нижних областей сайта и размещают свою рекламу мошеннические фирмы по продаже бесполезной, а иногда даже и вредной или опасной продукции сомнительного качества от неизвестных производителей.

Поэтому, если вы видите рекламу на нижней части сайта, будьте особенно внимательны и не доверяйте ей на 100%. Лучше всего проверить информацию о продукте или услуге на других сайтах или обратиться к экспертам. Не стоит покупать что-то только потому, что увидели рекламу на сайте с хорошей репутацией. Также следует обращать внимание на то, что скрывается за ссылками. Если вы переходите по ссылке, то проверьте адрес сайта и убедитесь, что это действительно тот сайт, который вы хотели посетить.

Приведем пример. С сайта primpress.ru из раздела «Новости партнеров» был произведен переход на страницу news-extra24.ru, при открытии которой нам открываются следующие предложения:

- некий 107-летний якобы известный кардиолог рекламирует для покупки лекарство для нормализации давления, причем не через аптечные сети, а именно через сайт «производителя», причем именно сегодня в течение нескольких часов действует скидка 100%, то есть препарат фактически отдается даром жителям определенного региона (https://blog-feed.org/solovyov-live-micardin/?channel=9mPq7G&click=605965154)

- другое предложение гласит о том, что на сверхвыгодных условиях предлагается чудо препарат, восстанавливающий зрение на 101% и сегодня в течение суток этот препарат можно заказать абсолютно бесплатно (https://cjknltxfsb.com....)

- третье предложение предлагает избавиться от спутниковой тарелки и бесплатно принимать 300 ТВ-каналов, купив некое чудо-устройство тысячи за 2-3 (https://cjknltxfsb.com...)

- четвертое предложение о призыве зарегистрироваться в информационной системе Quantum System, внести не менее 250$ начальный взнос, и буквально ничего не делая, получать баснословные деньги «из воздуха» благодаря уникальному ПО от Евгения Абрамова, работающего в сфере бинарных аукционов (quantumsys.ru и еще несколько зеркал этого сайта)

Список подобных примеров можно продолжать бесконечно. Данная статья ни в коем случае не ставит целью дискредитировать сайт primpress.ru, а только лишь в качестве примера поясняет, что многие региональные новостные сайты кроме информационно-осведомительской функции нередко могут являться площадками для размещения ссылок на паразитирующие сайты мо-

шенников.

Что отличает подобные сайты от безобидных одностраничников, продающих действительно полезные товары? Для всех этих сайтов характерно следующее: сначала идет много текста, часто в виде интервью с якобы известными людьми, которые подтверждают высокую эффективность данного продукта. Затем внизу большая кнопка при нажатии на которую открывается форма для ввода имени и фамилии заказчика и телефона. Никаких контактов на этих сайтах вы не найдете, как и информацию об учредительных документах фирмы. Звонить смогут только вам, но не вы сами. Как нетрудно догадаться основная задача подобных сайтов, а точнее «фирм», которых они представляют в сети – мотивация на покупку товаров сомнительного качества и неизвестного происхождения и таким, образом выманивание денег у частных лиц в основном с помощью методов социальной инженерии. Таким образом, даже если вы не купите товар, но зарегистрировались, то вам периодически будут звонить менеджеры фирмы и настойчиво уговаривать купить товар, ссылаясь на финансовые потери от вашего отказа и нередко угрожая судебным иском. И даже если человек не понесет прямых убытков, то его номер телефона останется в базе мошенников, который они могут в последствии перепродать другим мошенникам, работающих в других сферах, а это уже речь о потенциальной угрозе ИБ частного лица, поскольку по номеру телефона при желании можно идентифицировать личность человека и его цифровой профиль, что в свою очередь может привести к нарушению защиты персональных данных (ПДн).

К сожалению, сайтов первого и второго типа с каждым годом меньше не становится, а закона, запрещающего их деятельность или даже существование в сегменте Рунет пока нет. В этой связи резонно возникает вопрос: что можно предпринять в данной ситуации для того, чтобы сделать сетевой сегмент Рунет более чистым и информационно безопасным?

На наш взгляд возможно применить несколько различных подходов к повышению ИБ частных пользователей сетевого сегмента Рунет, о чем пойдет речь ниже. На данный момент авторы статьи предлагают к рассмотрению **6** таких подходов, каждый из которых имеет как свои плюсы, так и возможные минусы.

Если проблема является многофакторной и многоплановой, то в этом случае давно уже известен принцип «начни с себя». Речь идет о **цифровой** (информационной) **гигиене**, лежащей в основе первого подхода. Для ее реализации не являются обязательными какие-либо программно-аппаратные средства защиты, а значит этот подход является самым малозатратным с финансовой точки зрения. Для этого требуется прежде всего осведомленность человека о возможных киберугрозах и способах снижения вероятности их перехода в стадию инцидента. Главный принцип, который можно рекомендовать здесь – относиться с осторожностью и недоверием ко всему новому и ранее неизвестному, особенно, если речь идет о вводе своих персональных или банковских сведений. Для этого нужно периодически знакомиться с темати-

ческими дайджестами, в которых публикуются новые сведения об информационных угрозах и каналах их распространения, не игнорировать рекомендации специалистов по ИБ в вашей организации (для работающих). Основное преимущество данного подхода состоит в его простоте, а минус заключается в том, что эффективность защиты целиком зависит от уровня цифровой грамотности пользователя, который чаще всего формирует мнение об интернет-ресурсе субъективно или при недостаточной глубине анализа. В этом случае фейк-мейкеры и мошенники остаются безнаказанными.

Вторым принципиально другим подходом, а возможно и более эффективным является **создание нормативно правовой базы** с соответствующими законами. Так, например, можно ввести систему штрафов для владельцев сайтов, размещающих у себя ссылки или баннеры на сайты фейковой информации или ссылки на сайты мошенников, причем сумма штрафа должна быть выше, чем прибыль от размещаемых ссылок. У скептиков может возникнуть вопрос о том, как возможно оценить за короткий период времени большое количество сайтов рекламодателей – вручную это сделать будет сложно и дорого, т.к. возможно для этого потребуется большой штат веб-аналитиков. В этом случае можно рекомендовать внедрение систем искусственного интеллекта (СИИ), настроенных под данную задачу. Если разобраться, то отличить фейковую новость от настоящей можно путем поиска этой новости на сайтах агрегаторов или информационных агентств, которые официально зарегистрированы и известны, в т.ч. и региональных – эта задача вполне под силу искусственному интеллекту. То, что касается одностраничных сайтов мошенников – здесь тоже не так сложно применить систему искусственного интеллекта. Все подобные сайты имеют много общего, например: нечитаемые URL, форма для ввода контактов пользователя с таймером окончания акции, много текста вначале и фейковые отзывы, имитатор выигрыша с анимацией, да и сама структура одностраничного сайта уже может быть под подозрением. Все вышеперечисленное может быть включено в состав математической модели, которую будет использовать система искусственного интеллекта при анализе и блокировке сайта. Задача законодателей – обязать владельцев сайтов, сдающих свои фреймы в аренду иметь такие системы и штрафовать при их отсутствии, а возможно даже временно блокировать. В качестве альтернативы можно возложить эту функцию не на владельца сайта арендодателя, а, например, на Акционерное общество «Региональный Сетевой Информационный Центр», известный многим как «Ru-Center» [4]

Третьим подходом, который также относится к **нормативно правовым** может быть издание указа или закона, согласно которому Ru-Center перед регистрацией нового сайта проводит его экспертизу на предмет «информационной чистоты» и включает сайт в свой реестр с выдачей специального цифрового сертификата, подтверждающего благонадежность сайта. Причем этот сертификат должен быть доступен для просмотра любым пользователем при заходе на сайт. Учитывая большое количество ежедневно заявляемых сайтов, в помощь Ru-Center также может использоваться СИИ, работающая на тех же

принципах, что и в предыдущем подходе.

Подходы, основанные на нормативно правовых принципах, можно назвать своего рода цензурой или рецензированием, поскольку в их основе лежит анализ контента сайта.

Четвертый подход имеет совершенно другой принцип реализации. В его основе лежит **блокирование URL-адресов** сайтов фейковой информации и сайтов мошенников на уровне DNS-серверов провайдеров уровня Tier-2, которые по сути и составляют основу Рунета [5,6,7,8]. Но опять же приходим к тому, что нужна законодательная поддержка, обязывающая этих провайдеров иметь специализированные СИИ для автоматического анализа мошеннических сайтов и сайтов фейковой индустрии, поскольку вручную пронализировать такое количество сайтов ежедневно нереально.

Пятый подход не требует никакой нормативно-правой поддержки и заключается **в создании плагинов для наиболее используемых в России веб-браузеров**: Yandex, Google Chrome, Mozilla Firefox, Atom, Opera. Пользователь самостоятельно скачивает плагин и устанавливает его себе на компьютер или смартфон. Действие плагина может быть направлено на внесение соответствующих запретных IP-адресов в системный файл hosts, например, при первом обращении браузера к подозрительному сайту, либо непосредственно на браузер, в котором и будет происходить анализ страниц после отправки запроса на сервер сайта перед его закачкой в окно браузера. Подобные плагины уже существуют для блокировки навязчивой рекламы на сайтах [9,10,11]. Однако, в этом случае возможен негативный эффект - некоторое снижение скорости открытия страницы, поскольку для анализа потребуется какое-то время (впрочем, на достаточно производительных устройствах он может быть незначительным).

Некоторой разновидностью данного подхода может быть **создание и регулярное обновление БД неблагонадежных и мошеннических сайтов**, по аналогии с тем, как формируется БД спам-звонков в облачном сервисе Яндекс или лаборатории Касперского. В открытом доступе можно разместить файлы **hosts** с внесенными запретными IP-адресами. Пользователь скачивает себе этот файл и заменяет его на своем ПК в системной папке, причем даже этот процесс можно автоматизировать по аналогии с обновлением БД антивирусного ПО.

И шестой подход, который мы рассмотрим кардинально отличается от всех предыдущих по той причине, что он основан на одном из методов, используемых хакерами. Принцип состоит в том, чтобы регулярно, почти **постоянно совершать DDoS – атаки на сайты**, которые по критериям СИИ попадают в категорию мошеннических. В результате, сайт будет большую часть времени нефункционален, а значит иметь такой сайт мошенникам не будет никакого смысла. К возможным плюсам такого решения можно отнести предполагаемую эффективность, а к минусам – требуются специально выделенные сервера или мощные компьютеры, которые будут забрасывать мошеннический сервер запросами. Кроме того, в сетевом сегменте Рунет будет

много паразитного трафика, который может негативно сказаться и на работе легитимных сайтов.

Данная статья позволяет сделать два основных вывода:

1. для всех вышеописанных подходов требуется законодательная поддержка государства на внедрение систем искусственного интеллекта для автоматического анализа вредоносных сайтов, а также применение штрафных санкций для рекламодателя и / или арендодателя сайтового пространства (хостера) в случае отказа от таких систем или их ненадлежащей работы.

2. очевидна необходимость разработки СИИ для анализа сайтов и их внедрения для всех вышеописанных подходов.

В заключении отметим, что каждый из рассмотренных подходов требует дополнительных практических исследований и не может рассматриваться как абсолютная панацея для решения вышеописанной проблемы – обеспечение ИБ частных пользователей в сегменте Рунет, однако есть большая вероятность в том, что совокупность нескольких подходов позволит достичь гораздо большего эффекта, а значит сделать сегмент Рунет более безопасным и чистым для законопослушных пользователей.

Список литературы

1. Главные новостные сайты России [Электронный ресурс]. – URL: https://vsesmi.online/russia (дата обращения: 11.03.2023).
2. Статья. Желтая пресса в современной России [Электронный ресурс]. – URL: https://infopedia.su/17xf869.html (дата обращения: 11.03.2023).
3. Статья. Желтая пресса [Электронный ресурс] — URL: https://ru.wikipedia.org/wiki/Жёлтая_пресса (дата обращения: 11.03.2023)
4. Статья. Ru-Center [Электронный ресурс]. – URL: https://ru.wikipedia.org/wiki/Ru-Center (дата обращения: 11.03.2023)
5. Статья. На каких серверах держится Рунет? [Электронный ресурс]. – URL: https://news.rambler.ru/other/43670761-na-kakih-serverah-derzhitsya-runet/ (дата обращения: 11.03.2023)
6. Блог. Как дата-центры резервируют доступ в Интернет [Электронный ресурс]. – URL: https://www.xelent.ru/blog/kak-data-tsentry-rezerviruyut-dostup-v-internet (дата обращения: 11.03.2023)
7. Статья. Опорные сети Интернета [Электронный ресурс]. – URL: https://ru.wikipedia.org/wiki/Опорные_сети_Интернета (дата обращения: 11.03.2023)
8. Статья. Интернет-провайдеры разного уровня – принципы организации глобальной сети [Электронный ресурс]. – URL: https://asvagroup.com/2020/07/internet-provajdery-raznogo-urovnya-princzipy-organizaczii-globalnoj-seti (дата обращения: 11.03.2023)
9. Статья. Как блокировать рекламу в Яндекс браузере бесплатно: обзор блокираторов [Электронный ресурс]. – URL:

https://guidecomp.ru/luchshie-blokirovshhiki-reklamy-v-yandex-brauzere-na-android-i-windovs-rasshireniya-vstroennye-sredstva.html (дата обращения: 11.03.2023)
10. Статья. Лучшие антибаннеры. Блокировка рекламы [Электронный ресурс]. – URL: https://www.comss.ru/page.php?id=2621 (дата обращения: 11.03.2023)
11. Статья. Восемь лучших блокировщиков рекламы [Электронный ресурс]. – URL: https://lifehacker.ru/blokirovshhiki-reklamy (дата обращения: 11.03.2023)