

М.М. Шарипов

## ИССЛЕДОВАНИЕ reCAPTCHA ТРЕТЬЕЙ ВЕРСИИ

Рассматривается использование технологии reCAPTCHA с целью фильтрации и ограничения доступа к веб-сайту автоматизированных программ – ботов. Проводится исследование новой версии reCAPTCHA v3. Анализируются принципы работы алгоритма, на котором основывается новая версия.

*Ключевые слова:* фильтрация, бот, алгоритм, программа, reCAPTCHA, Интернет, решение.

М.М. Sharipov

## RESEARCH reCAPTCHA THIRD VERSION

The article discusses the use of reCAPTCHA technology in order to filter and restrict access to the website of automated programs – bots. A study of the new version of reCAPTCHA v3 is underway. The analysis of the principles of the algorithm on which the new version is base.

*Keywords:* filtering, bot, algorithm, program, reCAPTCHA, Internet, solution.

Развитие информационных технологий повлекло за собой появление в сети Интернет большого количества компьютерных программ, или так называемых ботов, которые выполняют заданные автоматически команды через пользовательский интерфейс, предназначенный для людей. Несмотря на то, что данные программы нашли широкое применение и используются для автоматического сбора и анализа данных о погоде, биржевых и валютных курсах, их использование нередко носит и вредоносный характер. Так, в настоящее время разработаны боты, которые способны скупить лучшие места на авиарейс, организовать DoS-атаки, зарегистрироваться на сайте, принимать непосредственное участие в онлайн-играх для фарминга игровой валюты, что приносит значительный материальный ущерб.

Для борьбы с цифровыми ботами в университете Карнеги – Меллон была разработана система, которая в сентябре 2009 г. была выкуплена компанией Google. Данная разработка получила название reCAPTCHA. Алгоритм системы строится на распознавании и вводе пользователем символов с картинки, так называемой «капчи». Применение данной технологии позволило не просто оградить веб-сайты от вредоносного влияния веб-ботов, но и оцифровывать книги, ранее находившиеся лишь на бумажных носителях (в 2011 г. reCAPTCHA выполняла оцифровку архивов газеты «The New York Times» и книг из Google Book Search). Google reCAPTCHA стала популярной системой для контроля отправки спам-контактных форм и злоупотребления трафиком на веб-сайтах.

С момента запуска системы защиты от ботов было представлено несколько версий программы.

1. reCAPTCHA v1 – ввод символов с картинки, чтение которых усложнено наложением дополнительных шумов, искажений, препятствующих автоматизации с помощью программных средств. При вводе символов важно учитывать раскладку клавиатуры

(русский/английский), а также символьный регистр. Данный вид проверки не всегда возможно пройти, так как часто исходные данные для ввода зашифрованы некорректно и вызывают проблемы у пользователей [1].

2. reCAPTCHA v2 – алгоритм основывается на проверке действий пользователя веб-ресурсом, при подозрении автоматизации действий предлагается решить «капчу». Как правило, в качестве задания предоставляется 9 изображений, среди которых необходимо выбрать только относящиеся к определенной тематике. Если же действия пользователя не вызывали сомнений, решение было доступно в один клик подтверждения «Я не робот» [1].

3. reCAPTCHA v3 – не требует взаимодействия с пользователем, т.е. проверка на основе анализа риска происходит в фоновом режиме. Система производит анализ cookie-файлов, ранее сохраненных в истории пользователя, отслеживает поведение и дает оценку действиям.

В настоящий момент представленная третья версия проходит бета-тестирование. Для разработчика доступен программный код, который необходимо прописать в своем сайте для использования и помощи в тестировании reCAPTCHA v3 [2].

Алгоритм проверки основывается на присвоении действиям пользователя численного значения в диапазоне от 1,0 до 0,0. Система проводит анализ каждого действия пользователя на веб-странице. На основе этого анализа проводится оценка. Для успешного распознавания в пользователе человека необходимо пройти порог в 0,3 балла. Если же это число ниже, то система определяет пользователя как автоматизированную программу, т.е. как бота. Так как система работает в фоновом режиме и при ее прохождении реальный пользователь может и не узнать о подключенной системе проверки, то целесообразно устанавливать код проверки сразу на несколько страниц для представления объективных данных и повышения качества распознавания. Структурного описания алгоритма, как происходит оценивание и дальнейшее действие, компания не разглашает.

Абнер Ли в 9to5Google считает, что основная цель разработчиков заключается в ранжировании оценок и выяснении, насколько подозрительно взаимодействие с пользовательским интерфейсом. При таком решении необходимость подключать пользователей к проблеме решения задач для дополнительной верификации сводится к минимуму [3].

При подключении технологии reCAPTCHA v3 к своему сайту в консоли администратора появляется информация о подозрительных активностях, оценках и другой объективной информации. Для подключения необходимо зарегистрировать свой сайт на странице reCAPTCHA и войти в систему с учетной записью Google, а затем потребуется произвести интеграцию системы, т.е. добавить необходимый код на сайт. Дальнейшие действия по блокировке активностей, не прошедших систему оценивания, производятся администратором сайта. Также можно установить, что сообщения о подозрительном трафике, зафиксированном с помощью Google reCAPTCHA, будут приходить на e-mail. Таким образом, администраторы теперь сами смогут управлять поведением reCAPTCHA на их сайте, когда раньше этим занимался Google. TechSpot выделяют три способа по настройке параметров reCAPTCHA [3].

1. Установить порог, который определяет, когда пользователь пропускается или когда должна быть проведена дополнительная проверка. Например, с использованием двухфакторной аутентификации и проверки телефона, проверки через e-mail.

## Шарипов М.М. Исследование reCAPTCHA третьей версии

2. Объединить систему оценивания с дополнительными сигналами, историей пользователя и транзакциями.

3. Использовать систему для машинного обучения уже установленной системы блокирования подозрительного трафика на веб-ресурсе.

Стоит отметить, что ранее взаимодействие и внесение дополнительных условий в алгоритм проверки были невозможны.

Для выявления всех возможностей новой версии reCAPTCHA проведем сравнительный анализ с предшествующими версиями.

**Сравнительный анализ возможностей версий reCAPTCHA**

	<b>reCAPTCHA V1</b>	<b>reCAPTCHA V2</b>	<b>reCAPTCHA V3</b>
Взаимодействие с пользователем	Происходит при вводе зашифрованного набора символов	Необходимое условие – выбрать набор изображений, относящихся к одной тематике	Происходит в фоновом режиме
Условие проверки	Безошибочный ввод символов с картинки	Подтверждение всех необходимых изображений	Проверка проходит на основе анализа рисков. Учитываются предыдущие сессии, блокируется подозрительный трафик
Установка на веб-сайт	Прописывается в место подтверждения формы	Установка в необходимое место на странице сайта	Скрипт устанавливается в любое место. Для точности проверки необходима установка на несколько страниц
Возможность интеграции с собственными методами проверки	Отсутствует	В зависимости от результата проверки предоставлять пользователю вариант решения задачи	После получения результатов анализа рисков администратор сам назначает дальнейшее действие для блокировки подозрительного трафика
Отчет о подозрительных активностях	Общая статистика	В консоли администратора	Структурированный отчет о каждом пользователе

После проведения сравнительного анализа было выявлено, что версия reCAPTCHA V3 включает в себя часть алгоритмов предшествующих версий, но при этом проверка происходит в фоновом режиме, что не отвлекает и не отпугивает пользователя. В новой версии reCAPTCHA появилось еще больше гибкости для настройки системы под свои нужды, что позволяет реализовать больше вариаций для использования на разных страницах сайта. При этом значительно улучшилось качество проверки, появилась возможность интеграции с собственными методами проверки. Вывод отчета в консоли администратора позволит строить график подозрительных активностей, применять дополнительные методы фильтрации.

Развитие современных информационных технологий не стоит на месте. С появлением новых разработок появляются методы их обхода. Несмотря на это, запуск версии reCAPTCHA V3 – это шаг к новому, инновационному методу фильтрации сети Интернет от вредоносных автоматизированных программ.

## Литература

1. *Аbrasimov M.B., Matorin A.A.* Анализ надежности графических captcha-систем на примере проекта reCAPTCHA // Математические основы интернет-безопасности [Электронный ресурс]. URL: <https://cyberleninka.ru/article/n/analiz-nadezhnosti-graficheskikh-captcha-sistem-na-primere-proekta-kcaptcha> (дата обращения: 10.04.2019).
2. *Habr* [Электронный ресурс]. URL: <https://habr.com/ru/company/globalsign/blog/415075/> (дата обращения: 26.02.2019).
3. *Zhang T.Y., Suen C.Y.* A fast parallel algorithm for thinning digital patterns // *Comm. ACM.* 1984. Vol. 27. № 3. P. 236–239.

## Literatura

1. *Abrasimov M.B., Matorin A.A.* Analiz nadezhnosti graficheskikh captcha-sistem na primere proekta reCAPTCHA // *Matematicheskie osnovy internet-bezopasnosti* [Elektronnyj resurs]. URL: <https://cyberleninka.ru/article/n/analiz-nadezhnosti-graficheskikh-captcha-sistem-na-primere-proekta-kcaptcha> (data obrashcheniya: 10.04.2019).
2. *Habr* [Elektronnyj resurs]. URL: <https://habr.com/ru/company/globalsign/blog/415075/> (data obrashcheniya: 26.02.2019).
3. *Zhang T.Y., Suen C.Y.* A fast parallel algorithm for thinning digital patterns // *Comm. ACM.* 1984. Vol. 27. № 3. P. 236–239.

DOI: 10.25586/RNUV9187.19.02.P.138

УДК 004.72

Р.Б. Сулейманов

---

ИССЛЕДОВАНИЕ ВОПРОСОВ МНОЖЕСТВЕННОГО ДОСТУПА  
В СИСТЕМАХ МОБИЛЬНОЙ СВЯЗИ С ИНТЕЛЛЕКТУАЛЬНЫМИ  
АНТЕННАМИ

---

Рассматривается использование технологий множественного доступа в системах мобильной связи. Особое внимание уделяется исследованию множественного доступа типа CDMA, который имеет широкую сферу применения и используется в системах с интеллектуальными антеннами.

*Ключевые слова:* система множественного доступа, канал связи, мобильная связь, передача сигнала, CDMA, интеллектуальная антенна.

R.B. Suleymanov

---

RESEARCH OF QUESTIONS OF MULTIPLE ACCESS  
IN MOBILE COMMUNICATION SYSTEMS WITH INTELLECTUAL  
ANTENNAS

---

The article discusses the use of multiple access technologies in mobile communication systems. Particular attention is pay to the study of multiple access type CDMA, which has a wide range of applications and is use in systems with intelligent antennas.

*Keywords:* multiple access system, communication channel, mobile communication, signal transmission, CDMA, intelligent antenna.