алгоритмы позволяют поставить в соответствие данным произвольного размера последовательность бит фиксированного размера, называемую хеш-значением. На основе результата сравнения хеш-значений, вычисленных для исходного и полученного сообщений, делается вывод о том, было ли сообщение модифицировано при его передаче по каналу связи.

В данной работе предложен алгоритм хеширования, основанный на использовании двумерных дискретных хаотических отображений [2]. Применение дискретных хаотических отображений позволяет сократить вычислительные затраты, необходимые на формирование хеш-значения. Предлагаемый алгоритм хеширования включает в себя следующие этапы: реализация итераций хаотических отображений с добавлением к переменным отображений элементов исходного сообщения и реализация итераций хаотических отображений без добавления элементов исходного сообщения. Проведено тестирование предлагаемого алгоритма при использовании следующих дискретных хаотических отображений: отображение «Кот Арнольда», отображение Чирикова, отображение пекаря. Установлено, что при использовании отображений Чирикова и пекаря для предлагаемого алгоритма характерен лавинный эффект, однако, при использовании отображения «Кот Арнольда» лавинный эффект отсутствует. Результаты анализа времени формирования хеш-значения свидетельствует о том, что для сообщений с размером большим 32 Кб предлагаемый алгоритм оказывается быстрее алгоритма «Keccak» более чем на 20 %.

Таким образом, предлагаемый алгоритм хеширования при использовании отображений Чирикова и пекаря может применяться при решении задач, связанных с контролем целостности данных при их передаче по различным каналам связи.

Литература

1. Криптология: учебник / Ю. С. Харин [и др.]. – Минск: БГУ, 2013. – 511 с.

2. Wong, K. Image encryption using chaotic maps / K. Wong // Intelligent computing based on chaos / L. Kocarev [et al] – Berlin, 2009. – Ch. 16. – P. 333–354.

ИСПОЛЬЗОВАНИЕ СЕРВИСА CLOUDFLARE ДЛЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ И ОТКАЗОУСТОЙЧИВОСТИ ВЕБ-ПРИЛОЖЕНИЙ

Г.И. Сидорин, Е.С. Кайгородова

С ростом количества и популярности веб-приложений остро встает вопрос обеспечения безопасности данных пользователей и их постоянной доступности. Необходимо, чтобы из любой точки планеты из любого устройства, поддерживающего соединение с интернетом, была возможность получить данные, при этом они должны быть надежно защищены от злоумышленников. Создание полноценной инфраструктуры для защиты содержимого веб-приложения, их масштабирования – это длительный и дорогостоящий процесс, требующий усилий и знаний гораздо больших, чем реализация основного функционала сервиса. Были проведены исследования по обеспечению безопасности с помощью облачных веб-сервисов. Наилучшие результаты по простоте использования, эффективности и стоимости показал сервис Cloudflare. Он предоставляет глобальную сеть доставки контента (CDN) с возможностями кеширования статического, ускорения динамического и оптимизации исходящего контента в зависимости от устройств, браузеров и пропускной способности. Благодаря этому веб-приложения отвечают пользователям максимально быстро, в какой точке планеты они бы ни находились. Также он предлагает бесплатную защиту SSL для шифрования веб-трафика в целях предотвращения кражи данных, повышения скорости загрузки веб-приложений и лучшей индексацией поисковыми движками. Атаки типа отказ в обслуживании (DoS) не являются недавним явлением, но методы и ресурсы, доступные для проведения и маскирования таких атак, резко эволюционировали. Cloudflare является одной из крупнейших сетей защиты от DDoS-атак в мире. С помощью его можно успешно бороться с атаками размером более 400 Гбит/с. Сервис предлагает бесплатные серверы доменных имен (DNS), которые являются одними из самых быстрых в мире. Cloudflare работает как обратный прокси-сервер и поддерживает множество новых протоколов: SPDY, HTTP/2, Websocket. Полученные результаты показывают целесообразность использования сервиса Cloudflare для обеспечения безопасности данных и отказоустойчивости веб-приложений. Такой способ особенно подойдет небольшим и средним веб-приложениям.