ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ТЕЛЕКОММУНИКАЦИИ
INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS

УДК 004.896

DOI: 10.21822/2073-6185-2025-52-3-126-134 Оригинальная статья/ Original article

Механизм защиты от DDoS–атаки типа Slowloris

П.В. Разумов, Л.В. Черкесова, Е.А. Ревякина
Донской государственный технический университет,
344000, г. Ростов-на-Дону, пл. Гагарина, 1, Россия

Резюме. Цель. Целью исследования является программный анализ кибератаки Slowloris и реализация механизма защиты от DDoS–атаки типа Slowloris. **Метод.** Для разработки программного средства был выбран язык программирования PHP, так как данный язык зарекомендовал себя как один из самых популярных и широко используемых языков в веб-разработке. Вместе с языком программирования была выбрана IDE PhpStorm от компании JetBrains. **Результат.** Разработан программный механизм защиты от DDoS–атаки типа Slowloris. Механизм имеет ряд преимуществ по сравнению с аналогами: возможность использовать программное средство бесплатно, возможность модификации; соответствует требованиям к надежности пароля по современным стандартам; использование HTTPS протокола для защищенного соединения; шифрование запросов; хеширование пользовательских данных авторизации (login, password) и хранение на сервере в БД и др. **Вывод.** Разработанное программное средство можно использовать как встраиваемый механизм защиты любых страниц авторизации или регистрации, позволяющее автоматически блокировать потенциально опасные соединения.

Ключевые слова: Slowloris, DDoS–атака, механизм, защита, алгоритм

Для цитирования: П.В. Разумов, Л.В. Черкесова, Е.А. Ревякина. Механизм защиты от DDoS–атаки типа Slowloris. Вестник Дагестанского государственного технического университета. Технические науки. 2025; 52(3):126-134. DOI:10.21822/2073-6185-2025-52-3-126-134

Slowloris DDoS Defense Mechanism

P.V. Razumov, L.V. Cherkesova, E.A. Revyakina
Don State Technical University,
1 Gagarin Square, Rostov-on-Don 344000, Russia

Abstract. Objective. The objective of this study is to perform a software analysis of the Slowloris cyberattack and implement a protection mechanism against a Slowloris-type DDoS attack. **Method.** PHP was chosen for the development of the software tool, as it has established itself as one of the most popular and widely used languages in web development. The PhpStorm IDE from JetBrains was also selected along with the programming language. **Result.** A software mechanism for protection against a Slowloris-type DDoS attack has been developed. The mechanism has several advantages over similar approaches: the software can be used free of charge and is modifiable; it meets modern password strength requirements; it uses the HTTPS protocol for secure connections; it encrypts requests; it hashes user authorization data (login, password) and stores it in a database on the server, etc. **Conclusion.** The developed software tool can be used as an embedded protection mechanism for any authorization or registration pages, allowing for the automatic blocking of potentially dangerous connections.

Keywords: Slowloris, DDoS attack, mechanism, protection, algorithm

For citation: P.V. Razumov, L.V. Cherkesova, E.A. Revyakina. Slowloris DDoS Defense Mechanism. Herald of Daghestan State Technical University. Technical Sciences. 2025;52(3):126-134. (In Russ) DOI:10.21822/2073-6185-2025-52-3-126-134

Введение. В настоящее время существует большое количество атак, направленных на интернет-ресурсы и серверы. К тому же, проблема защиты от кибератак наиболее

актуальна в период кибервойн и кибертерроризма, так как они направлены на ключевые топливно-энергетические компании.

Проблема DDoS атак на данный момент является очень актуальной в России, ведь за 2022 год количество атак данного типа по сравнению с показателями годичной давности выросло на 700 процентов. В первую очередь атакуются госорганизации и крупные корпорации. Так 21 октября 2022 года атакой по типу Slowloris были атакованы сервера крупной российской компании «Газпром», и в результате данной кибератаки сервера были отключены не менее месяца. Потери при такой атаки только на восстановление составят не менее 35 миллионов рублей. Также из-за DDoS–атак были отключены Web–сайты Роскосмоса, Госуслуг, Роспотребнадзора и другие. 21 июня 2022 года лабораторией Касперского была зафиксирована самая длинная DDoS–атака, которая длилась 29 дней, можно только догадываться какими могут быть убытки при таких продолжительных атаках на крупные корпорации, особенно в ТЭК.

Постановка задачи. Целью настоящего исследования является программный анализ кибератаки Slowloris и реализация механизма защиты от DDoS–атаки. Объектом исследования является кибератака DDoS–атака типа Slowloris. Предметом исследования являются механизмы защиты от DDoS–атака типа Slowloris.

Методы исследования. Атака Slowloris, или как ее еще называют, сессионная атака, хоть и не является сравнительно новой, при этом очень «перспективна», ведь трафик такой атаки тяжело обнаружить, так как по сравнению с другими DDoS–атаками он мал. Открывая множество соединений, хакер держит их как можно дольше открытыми, что н не дает возможности другим пользователям подключить к ресурсу.

Так что же такое DoS и DDoS–атаки? Атаки типа «отказ в обслуживании» являются разновидностью сетевых атак. Сетевые атаки удалённого доступа, в свою очередь, подразделяются на следующие категории: сниффер–пакеты; IP-спуфинг; отказ в обслуживании; парольные атаки; атаки вида человек по середине; атаки на уровне приложений; сетевая разведка; злоупотребление доверием; переадресация портов; несанкционированный доступ; вирусы и приложения типа «Троянский конь».

В большинстве своем DoS–атака – это кибератака, направленная на сервер жертвы, отправляя большой информационный поток, полностью занимает его ресурс из-за чего он не может обрабатывать запросы обычных пользователей. DDoS–атака является продолжением развития DoS–атаки и отличается только тем, что злоумышленник атакует не с одного устройства, а с некоторого количества (сети) устройств, и при этом количество устройств ограничено только ресурсами злоумышленника. Такие атаки представлены схематически (рис. 1, 2).

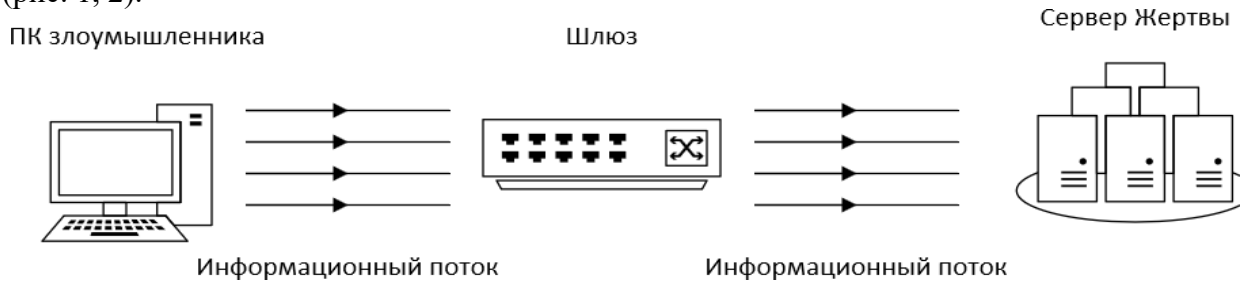

Рис. 1 – DoS атака
Fig. 1 – DoS attack

DDoS–атаки является очень популярным механизмом причинения вреда различным интернет структурам у злоумышленников, в связи с этим с каждым днем появляются все новые виды атак этого типа, задействую при этом различные уровни модели OSI, такие как второй уровень – канальный, третий уровень – сетевой, четвертый уровень – транспортный и седьмой уровень – прикладной. При этом данные атаки в основным классифицируют по механизму действия, подробная классификация приведена в табл. 1 [1].

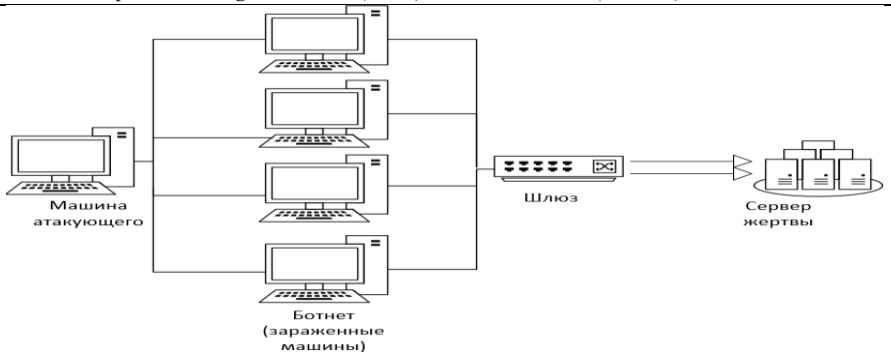

Рис. 2 – DDoS атака
Fig. 2 – DDoS attack

Средствами распределенных атак по типу отказа в обслуживании являются ботнеты и выделенные сервера. Выполнение DDoS–атаки можно рассчитать по простой формуле. DDoS = (количество устройств) * (производительность) * (скорость и качество соединения). Но нельзя забывать, что вычислительные мощности растут и, в связи с этим цена атаки уменьшается, а мощность увеличивается. При этом по статистике проведенных DDoS–атак в России страдают множество разных отраслей.

Таблица 1. Виды DDoS–атак
Table 1. Types of DDoS attacks

DDOS атаки по механизму действия						
Переполнение канала		Использование уязвимостей протоколов			Атака на уровне приложений	Другие
DNS/NTP амплификация	Фрагментированный ACK/UDP/ICMP флуд	SYN/ PUSH ACK/RST/SYN-ACK/ACK/FIN флуд	DRDoS	DNS reflected Amplification	HTTP флуд	Pulse Wave
APDoS	Флуд медиа-данными	IP null / TCP null атака	Ping смерти (POD)	Атаки с модификацией поля TOS	Атака с целью отказа приложения	Yo-yo
Атака широковещательными ICMP ECHO/ UDP пакетами	Burst attack (Hit-and-run)	Атака поддельными TCP сессиями с несколькими (или без) SYN-ACK/ACK	SSDP	Атака с подменой адреса отправителя адресом получателя	Атака медленными сессиями SlowLoris/SlowDroidRUDY	CPDoS
Challenge Collapsar	Nuke	Каплевидная атака	UPnP	Smurf-атака	Атака фрагментированными HTTP пакетами	Phlashing (PDOS)
ICMP/NTP/Ping/UDP/DNS/VoIP/MAC флуд		Атака помощью перенаправления трафика высоко нагруженных сервисов			XML DoS	TDoS

Атаки медленными сессиями выполняются на седьмом уровне оси с использованием HTTP запросов, а именно суть данной атаки в отправке GET запроса с незакрытым заголовком, открывая все больше и больше соединений, при этом периодически добавляя еще HTTP заголовки, но не завершая процесс.

Большое влияние атаки данного типа оказывают на серверы плохо обрабатывающие тысячи соединений, такие как Apache и меньшее влияние varnish и nginx. При этом есть сервера более устойчивые к данной атаке за счет своей конструкции, например, Hiawatha и Cisco Css.

Существующие методы защиты постоянно совершенствуются, но ни одно средство не может дать полной гарантии на защиты от атаки типа отказ в обслуживании, такие большие информационные потоки мало какие сервера смогут корректно обрабатывать при этом не задействую все вычислительные способности только на нелегальном трафике.

Рассмотрим уже существующие механизмы защиты от DDoS–атак. Стоит отметить, что количество таких программ постоянно, все они имеют особенности, и более подробно методы приведены в табл. 2.

Таблица 2. Способы защиты от DDoS–атак
Table 2. Methods of protection against DDoS attacks

Механизмы защиты от DDoS–атак **Methods of protection against DDoS attacks**						
Фильтрация Filtration		По ресурам By resources			Безопасность подключения Connection Security	
Пакеты Packages	Потоки Streams	Изменение количества ресурсов Changing the amount of resources	Перенос ресурсов Transfer resources	Разграничение ресурсов Resource delimitation	SSL/TLS	Шифрование запросов Encrypting requests

Рассматривая тип атаки Slowloris нужно правильно защищаться от всевозможных атак, реализуемых посредством HTTP – запросов и ботами, и различными программными средствами по перебору паролей. При этом самый простой метод защиты от HTTP – атак это переход на безопасное SSL / TLS соединение посредством протокола HTTPS и использование внутреннего шифрования запросов с использованием симметричных шифров. Так же не стоит забывать, что данный вид атаки тяжело отслеживается, ведь его трафик в сравнении с другими DDoS–атаками сравнительно мал, что создает не мало трудностей. При этом для смягчения данной атаки желательно использовать только те сервера, которые хорошо обрабатывают тысячи подключений, или конструктивно более устойчивые конкретно к этой атаке. Методы смягчения подробно рассмотрены в табл. 3.

Таблица 3. Методы смягчения атаки Slowloris
Table 3. Slowloris attack mitigation methods

Методы защиты Methods of protection		
Снижение таймаута на ожидание ответного пакета Reducing the timeout for waiting for a response packet	Ограничение на количество сессий с одного адреса или подсети Limit on the number of sessions from one address or subnet	Ограничение на минимальную скорость передачи Minimum transfer rate limit
Увеличение максимального числа клиентов Increasing the maximum number of clients	Использование менее подверженного сервера Using a less vulnerable server	Настройка обратных прокси серверов Setting up reverse proxy servers
Настройка брандмауэров Setting up firewalls	Настройка коммутаторов контента Setting up content switches	Настройка балансировщиков нагрузки Configuring load balancers
Использование модулей для серверов регулирующие их работу с сессиями Using modules for servers that regulate their work with sessions		

Рассматривая методы борьбы с сессионными атаками можно заметить, что одними из самых распространенных и перспективных являются атаки медленной сессии, такие как Slowloris. Для того чтобы обезопаситься от данной атаки рассмотрим следующие подходы:

1. Переход от стандартного протокола HTTP на HTTPS. Https – расширение протокола передачи данных (HTTP) который обеспечивает шифрование соединения, что, в свою очередь, защитит от прослушивания сетевого соединения и затруднит атаки, реализующиеся с помощью POST и GET - запросов.
2. Использование внутреннего шифрования POST и GET запросов, посредством симметричного алгоритма шифрования, что обезопасит передачу данных пользователя.
3. Хранение учетных данных пользователей в хешированном виде; в случае перехвата данных, злоумышленник не сможет ими воспользоваться без предварительной расшифровки.
4. Реализация анализа трафика и блокирование потенциально опасных подключений, для защиты от ботов и атак с распределённых устройств.
5. Использование сервера, имеющем в своем функционале работу с тысячами соединений.
6. Использование модулей, регулирующих работу сессиями. Многие разработчики, зная о таких атаках выпускают дополнительные модули для серверов, ограничивающие время работы одной сессии и скорость подключения, например,

для Apache – mod_limitipconn, mod_qos, mod_evasive, безопасность модов, mod_noloris и mod_antiloris, что снизит вероятность успешного выполнения данной атаки.

7. Использование скрипта, который проверяет количество подключений с IP-адреса отдельного источника; просматривает журналы приложений и определяет сеансы, прошедшие проверку подлинности, и, следовательно, IP-адресов клиентов, прошедшие проверку подлинности; сообщает об IP-адресах клиентов, превышающих лимиты подключений; настраиваемые ограничения: количество подключений на одного клиента, продолжительность индивидуального подключения.

Используя данные методы и способы смягчения проведения атак медленными сессиями получим следующую схему работы web-сервиса (рис. 3).

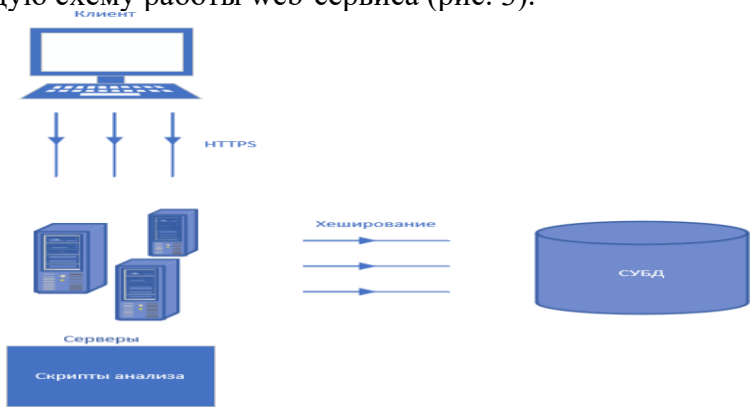

Рис. 3 – Схема сервиса
Fig. 3 – Service scheme

Использование данных методов и способов защиты позволит не только защитить сервис от атак различного вида, таких как атаки посредством HTTP – запросов, так сделать невозможным или смягчить воздействие атак медленными сессиями на сервера.

Обсуждение результатов. Для разработки программного средства был выбран язык PHP, так как данный язык зарекомендовал себя как один из самых популярных и широко используемых языков в веб-разработке. Вместе с языком программирования была выбрана IDE PhpStorm от компании JetBrains. Данная компания выпускает продукты практически для всех популярных на данный момент языков программирования, так же ее продукты зарекомендовали себя как многофункциональные и удобные IDE для разработки и ведения контроля версий. Помимо данного языка использовались языки верстки CSS и JS, язык разметки HTML.

PHP - скриптовый язык общего назначения, интенсивно применяемый для разработки веб-приложений. В настоящее время поддерживается подавляющим большинством хостинг-провайдеров и является одним из лидеров среди языков, применяющихся для создания динамических Web–сайтов. Является сравнимо быстрым языком, сравнивая с более популярным Python и более молодым Golang, является удобным и сравнимо быстрым, хоть и использует интерпретатор. В качестве базы данных было использовано современное СУБД MySQL на базе программного пакета MAMP.

Разработанное в ходе данного исследования программное средство можно использовать как встраиваемый механизм защиты любых страниц авторизации или регистрации.

Программное средство соответствует следующим требования к надежности:

- требования к надежности пароля по современным стандартам;
- использование HTTPS протокола для защищенного соединения;
- шифрование запросов с помощью симметричного алгоритм шифрования, в данном случае, AES 256;
- хеширования пользовательских данных авторизации (login, password) и хранение на сервере в БД;
- автоматическое блокирование потенциально опасных соединений.

Написанный алгоритм шифрования AES 256 из предыдущих работ, в которых сравниваются временные характеристики данного алгоритма, написанного на разных языках программирования [2]. На рис. 4 приведена структура данного алгоритма [3]:

```
class Aes
{
    // основная ф-я шифрования
    public static function cipher($input, $w)
    {
        $Nb = 4; //
        $Nr = count($w) / $Nb - 1; // количество раундов: 10/12/14 для ключей 128/192/256-бит

        $state = [];  // 4xNb state
        for ($i = 0; $i < 4 * $Nb; $i++) {
            $state[$i % 4][floor( num: $i / 4)] = $input[$i];
        }

        $state = self::addRoundKey($state, $w,  rnd: 0, $Nb);

        // применить Nr раундов
        for ($round = 1; $round < $Nr; $round++) {
            $state = self::subBytes($state, $Nb);
            $state = self::shiftRows($state, $Nb);
            $state = self::mixColumns($state, $Nb);
            $state = self::addRoundKey($state, $w, $round, $Nb);
        }

        $state = self::subBytes($state, $Nb);
        $state = self::shiftRows($state, $Nb);
        $state = self::addRoundKey($state, $w, $Nr, $Nb);
```

Рис. 4 – Алгоритм AES
Fig. 4 – AES algorithm

Схема реализации шифрования POST и GET запросов представлена на рис. 5:

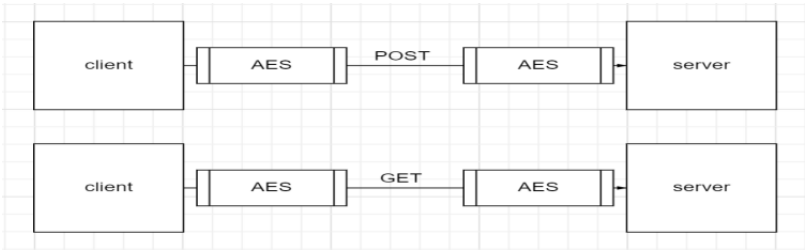

Рис. 5 – Схема шифрования запросов
Fig. 5 - Request ciphering scheme

Программное средство реализующие анализ соединений и занесений ip-адресов в черный список было реализовано в двух файлах main.php и black_list.db.

Основные функциями программы являются: функция конфигурации; функция параметров; монитор подключений; функция сбора и анализа статистики; главная функция закрытия соединений и занесения в черный список ip-адресов. Блок схема алгоритма программного средства представлена на рис. 6.

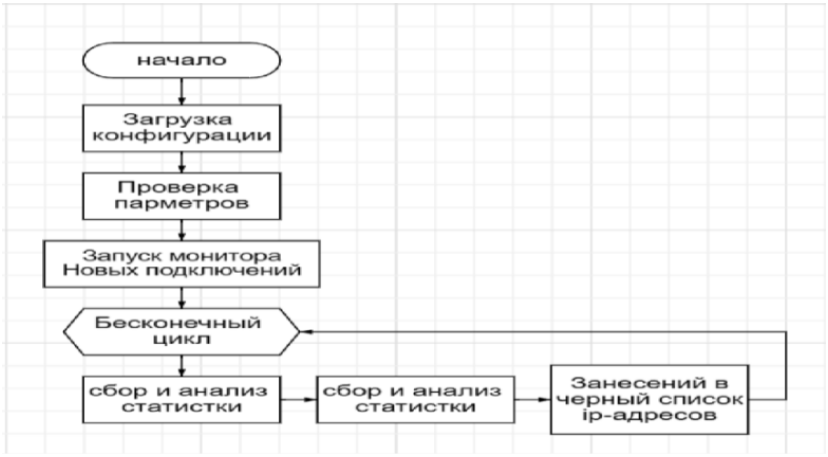

Рис. 6 – Блок-схема программного средства
Fig. 6 – Block-scheme of software

Также реализован скрипт, который отслеживает соединения и сеансы приложений для поддержки защиты от DDoS–атак на уровне приложений. Часть скрипта, а именно, вызов основных исполняемых функций представлена на рис. 7.

```
vprint "Loading configuration"
exit 1 if load_config()

vprint "Starting parameter checking"
exit 1 if (check_parameters)

vprint "Starting monitor for new connections"
start_new_connection_monitor()

vprint "Starting monitor for new logins"
start_new_login_monitor()

vprint "Starting main loop"
```

Рис. 7 – Основное тело программного средства
Fig. 7 – Main part of software

Механизм работы. Хранение пароля в базе данных в шифрованном виде реализовано с помощью хеш-функции sha256. [4]. Использование данной хеш-функции является важным аспектом безопасности, она является современным и криптостойким решением на сегодняшний день. Сравнивая ее с sha512, по криптостойкости они будут примерно равный, но при этом другие достаточно известные решения такие как md5 и sha1 использовать уже не целесообразно, так как они уже были взломаны [5]. Выполнение программного модуля на kali linux на рис. 8. По выполнению видно, что атака выполняется корректно, при этом занимая указанное количество сокетов веб сервиса.

```
[24-01-2023 00:58:39] Attacking 127.0.0.1 with 500 sockets.
[24-01-2023 00:58:39] Creating sockets...
[24-01-2023 00:58:39] Sending keep-alive headers...
[24-01-2023 00:58:39] Socket count: 500
[24-01-2023 00:58:54] Sending keep-alive headers...
[24-01-2023 00:58:54] Socket count: 500
[24-01-2023 00:59:09] Sending keep-alive headers...
[24-01-2023 00:59:09] Socket count: 500
```

Рис. 8 – Выполнение Slowloris
Fig. 8 – Slowloris execution

На рис. 9 показано попытка открытия страницы локального сервера, на который произведена атака, можно заметить, что данные не получаются и страница при этом не загружается.

Рис. 9 – Успешное выполнение атаки и заморозка сервиса
Fig. 9 – Succesful attack

При этом с использованием программного средства и при проведении атаки на тоже количество сокетов, сервер работает стабильно нормально передает данные к пользователю и можем видеть на рис. 10, успешное получение данных и загрузку страницы.

Рис. 10 – Успешная загрузка страницы
Fig. 10 – Successful webpage loading

Данный механизм имеет ряд преимуществ по сравнению с аналогами:

- возможность использовать программное средства бесплатно;
- имеет перспективу в модификации. Как важный аспект, данный механизм можно дорабатывать, улучшать скрипты и добавлять свои методы защиты, чтобы улучшить защиту от различный кибератак;
- не нагружает систему. Так как все используемые средства встроены в локальный Web–сайт и работают на достаточно быстром языке программирования.
- не занимает много места, так как весь механизм легко разработчиками может быть встроен в любой Web–сайт.

– может работать совместно с другими программами, что позволит защищаться от компьютерных атак различного типа.

Таким образом можно сделать вывод, что механизм защиты использует современные требования к обеспечению безопасности пользовательских данных, успешно справляется с защитой от атак медленными сессиями или, по крайней мере, смягчает их воздействие, а также несколько других DOS – атак.

Общие рекомендации по защите от атак по типу отказ в обслуживании. Существует ряд рекомендаций, которым пользователю следует придерживаться, чтобы защитить себя от DOS – атак [6]:

1. Уменьшение зон, доступных для атаки. Этого можно добиться, ограничив доступ к портам, протоколам или приложениям, взаимодействие с которыми не предусмотрено, в том числе ограничить интернет-трафик к серверам.
2. Сведения о типичном и нетипичном трафике. Сбор сведений о нетипичном и трафике, его анализ и блокировка потенциально опасного.
3. Использование безопасного подключения HTTPS, как способ защиты от HTTP флуда, а также сторонних механизмов защиты от различных спам и флуд атак, реализующиеся в том числе и ботами [7].
4. Развертывание брандмауэров для отражения сложных атак уровня приложений. Использование межсетевых экранов позволит противодействовать попыткам внедрения SQL – кода или подделки межсетевых запросов, а также фильтрация и ограничение трафика и работу сторонних приложений.
5. План масштабирования. В данном пункте необходимо выделить два элемента: пропускная способность и производительность сервера. Пропускная способность (транзитивный потенциал) – необходимо размещать ресурсы в непосредственной близости с конечными пользователями и крупными узлами межсетевого обмена трафиком. Производительность сервера – чем лучше производительность сетевых интерфейсов и сетевая конфигурация, тем лучше будет происходить обработка больших объемов трафика.
6. При защите от атак медленными сессиями, использовать сервера рассчитанные на тысячи подключений такие на nginx или varnish. Так же нельзя забывать про настройку серверов по времени ожидания и минимальной скорости подключения, либо использование готовых модулей от разработчиков серверов для снижения вероятности успешного выполнения атаки медленными сессиями.
7. Для смягчения сессионных атак, таких как Slowloris и SlowDroid, использовать умные фильтры или программные средства отслуживающие в режиме реального времени все подключения на наличие опасного трафика исходящего от определенных IP-адресов или узла, и блокировка таких подключений во избежание отказа в обслуживание.

Вывод. Проведено исследование компьютерных атак; разработана программная реализация механизма защиты. Проведен сравнительный анализ реализованного механизма защиты с аналогами и модификациями. Тестовая среда, используемая для атаки, не смогла обмануть программное средство. Тестирование прошло успешно, что доказывает о правильности работы расширения и возможности в перспективе модификации.

Проведенное исследование еще раз доказывает, что каждый пользователь должен себя обезопасить от любых несанкционированных угроз, поэтому проанализированы наиболее распространенные типы кибератак, приводящие к блокировке учетных записей, а также представлены общие рекомендации по защите от DDoS–атак и их разновидности, а именно, сессионных атак.

Представленный в статье механизм защиты является современным решением, обеспечивающим защиту от атак медленными сессиями. Как минимум, механизм сильно смягчает последствия DDoS–атаки типа Slowloris.

Библиографический список:

1. Razumov P.V., Safaryan O.A., Cherckesova L.V., et all. “Developing of Algorithm of HTTP Flood DDoS Protection”, IEEE 3rd International Conference on Computer Applications & Information Security, IEEE ICCAIS’20. Saudi Arabia, Er-Riyadh, 2020. pp. 1 – 6.
2. Стариков А.А., Лысенко А.В, Клевцов А.А. “Разработка и анализ скорости работы блочного симметричного алгоритма шифрования AES с использованием различных языков программирования” / Молодой исследователь Дона, № 4 (37) 2022. С. 38 – 41.
3. Dong X., Sun S., Shi D. Quantum Collision Attacks on AES-like Hashing with Low Quantum Random Access Memories, Advances in Cryptology - ASIACRYPT-2020, South Korea, Daejeon, Springer International Publishing, Vol. 12492, pp.727-757 doi: 10.1007/978-3-030-64834-3
4. Al-Odat Z., Abbas A., Khan S. Randomness Analyses of the Secure Hash Algorithms, SHA-1, SHA- 2 and modified SHA, 2019 International Conference on Frontiers of Information Technology (FIT), 2019. Pp. 3160-3165. doi: 10.1109/FIT47737.2019.00066
5. Karthiga S. Velmurugan T. Security based Approach of SHA-384 AND SHA-512 Algorithms in Cloud Environment, *Journal of Computer Science*, 2019; 16(10):1439-1450. DOI: 10.3844/jcssp.2020.1439.1450
6. Razumov P., Lyashenko K., Cherckesova L., Revyakina E., etc. Development of a System for Protecting against DDoS Attacks at the Level of the OSI Model – HTTP Flood / TransSiberia 2023, E3S Conferences 402, 03008 (2023), Pp 1 – 9, https://doi.org/10.1051/e3sconf/202340203008.
7. Alzahrani, S. and Hong, L. Generation of DDoS Attack Dataset for Effective IDS Development and Evaluation. Journal of Information Security 2018, 9, 225-241 DOI: 10.4236/jis.2018.94016

References:

1. Razumov P.V., Safaryan O.A., Cherckesova L.V., et all. “Developing of Algorithm of HTTP Flood DDoS Protection”, IEEE 3rd International Conference on Computer Applications & Information Security, IEEE ICCAIS’20. Saudi Arabia, Er-Riyadh, 2020:1 – 6.
2. Starikov A.A., Lysenko A.V., Klevtsov A.A. “Development and analysis of the performance of the block symmetric encryption algorithm AES using various programming languages”. *Young researcher of the Don*, 2022; 4 (37): 38 – 41. (In Russ)
3. Dong X., Sun S., Shi D. Quantum Collision Attacks on AES-like Hashing with Low Quantum Random Access Memories, Advances in Cryptology - ASIACRYPT-2020, South Korea, Daejeon, *Springer International Publishing*, Vol. 12492, Pp.727-757 doi: 10.1007/978-3-030-64834-3
4. Al-Odat Z., Abbas A., Khan S. Randomness Analyses of the Secure Hash Algorithms, SHA-1, SHA-2 and modified SHA, 2019 International Conference on Frontiers of Information Technology (FIT), 2019: 3160-3165. doi: 10.1109/FIT47737.2019.00066
5. Karthiga S. Velmurugan T. Security based Approach of SHA-384 AND SHA-512 Algorithms in Cloud Environment, *Journal of Computer Science*, 2019;16(10):1439-1450. doi: 10.3844/jcssp.2020.1439.1450
6. Razumov P., Lyashenko K., Cherckesova L., Revyakina E., etc. Development of a System for Protecting against DDoS Attacks at the Level of the OSI Model – HTTP Flood / TransSiberia 2023, E3S Conferences 402, 03008 (2023), Pp 1 – 9, https://doi.org/10.1051/e3sconf/202340203008.
7. Alzahrani, S. and Hong, L. Generation of DDoS Attack Dataset for Effective IDS Development and Evaluation. Journal of Information Security 2018;9:225-241 DOI: 10.4236/jis.2018.94016

Сведения об авторах:

Разумов Павел Владимирович, аспирант, кафедра «Кибербезопасность информационных систем»; razumov1996@inbox.ru; ORCID0000-0003-2454-3600

Черкесова Лариса Владимировна, доктор физико-математических наук, профессор, профессор, кафедра «Кибербезопасность информационных систем»; chia2002@inbox.ru

Ревякина Елена Александровна, кандидат технических наук, доцент, доцент, кафедра «Кибербезопасность информационных систем»; Revyelena@yandex.ru

Information about authors:

Pavel V. Razumov, Postgraduate Student, Department of Cybersecurity of Information Systems; razumov1996@inbox.ru; ORCID0000-0003-2454-3600

Larisa V. Cherkesova, Dr. Sci. (Physics and Mathematics), Prof., Prof., Department «Cybersecurity of information Systems»; chia2002@inbox.ru

Elena A. Revyakina, Cand. Sci. (Eng.), Assoc. Prof., Assoc. Prof., Department «Cybersecurity of information systems»; Revye-lena@yandex.ru

Конфликт интересов/Conflict of interest.

Авторы заявляют об отсутствии конфликта интересов/The authors declare no conflict of interest.

Поступила в редакцию/ Received 08.04.2025.

Одобрена после рецензирования/ Reviced 20.05.2025.

Принята в печать/ Accepted for publication 19.07.2025.