МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ОБРАЗОВАНИЯ «ДОНСКОЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ» (ДГТУ)

Разработка и анализ эффективности средств противодействия от DDoS-атак

Научный руководитель
д.ф-м.н., профессор
Черкесова Лариса Владимировна

Выполнил
студент группы ВКБ61
Разумов Павел Владимирович

Цель исследования:

Разработка защитного механизма противодействия распределенным DoS-атакам типа HTTP Flood, основанный на методе проксирования запросов в клиент-серверной сетевой архитектуре

Объект исследования:

Информационная система, подверженная DDoS – атакам посредством организации распределенной сети ботнет, и методы их отражения

Предмет исследования:

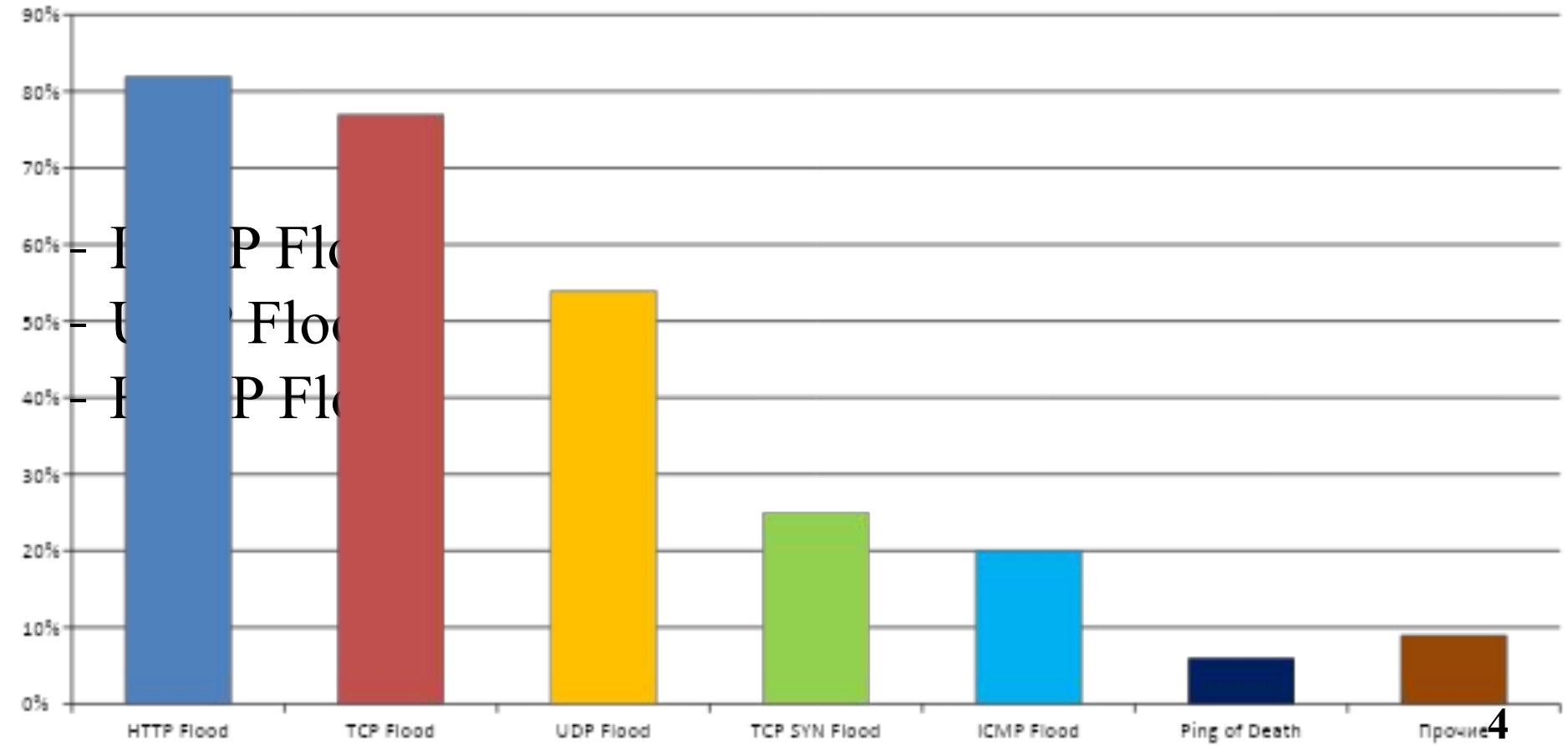
Защитный механизм противодействия DDoS-атакам HTTP Flood, совершаемым на уровне L7 модели OSI

Задачи исследования:

- *исследование возможных DDoS-атак и их классификация;*
- *анализ* особенностей реализации атак типа DDoS, в особенности, атаки HTTP flood;
- *разработка алгоритма* противодействия атакам HTTP Flood на уровне L7 модели OSI;
- *программная реализация* разработанного алгоритма отражения атак;
- *тестирование* работы алгоритма распознавания и отражения DDoS-атак HTTP Flood.

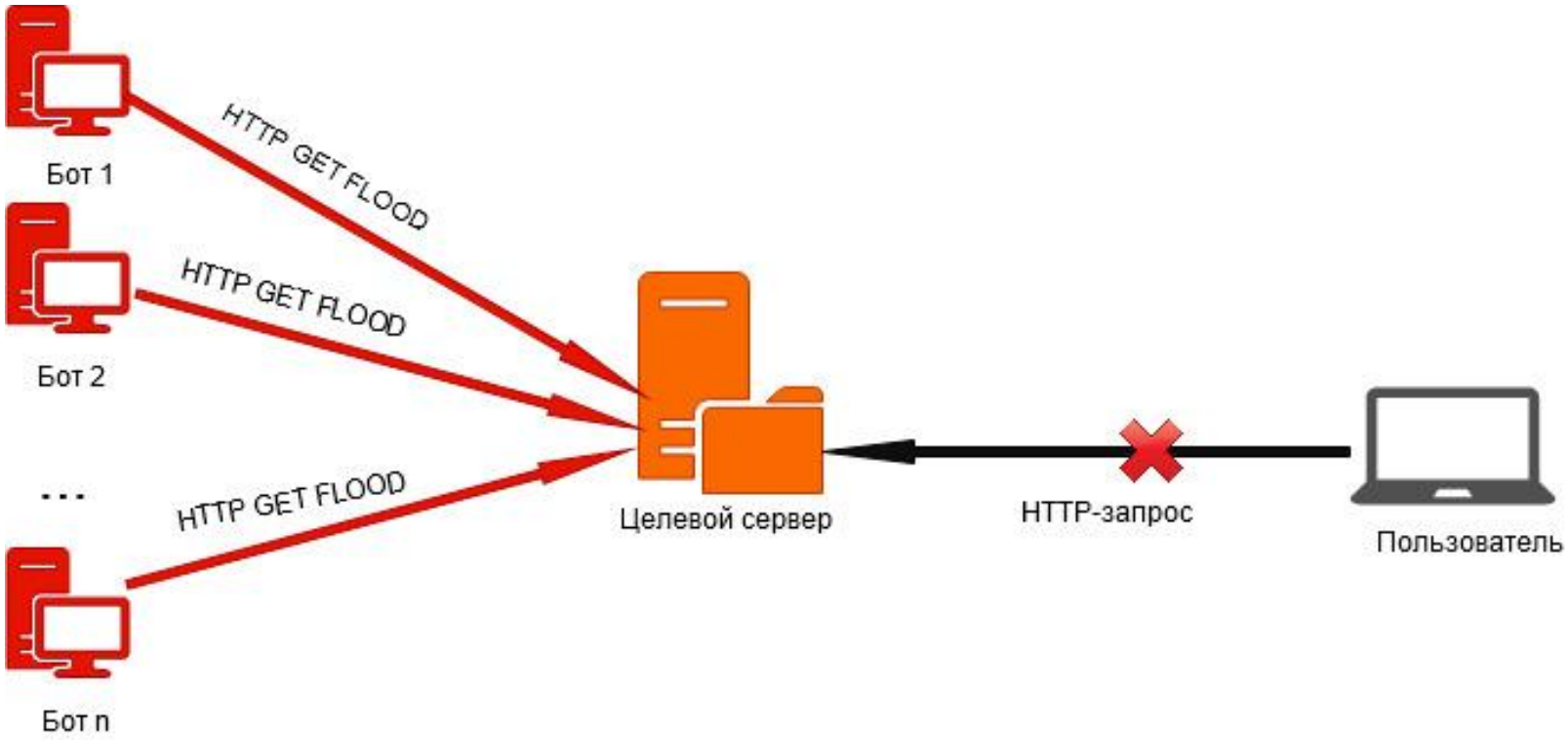
Наиболее распространенные DDoS-атаки

- TCP SYN Flood;
- TCP Flood;
- Ping of Death;



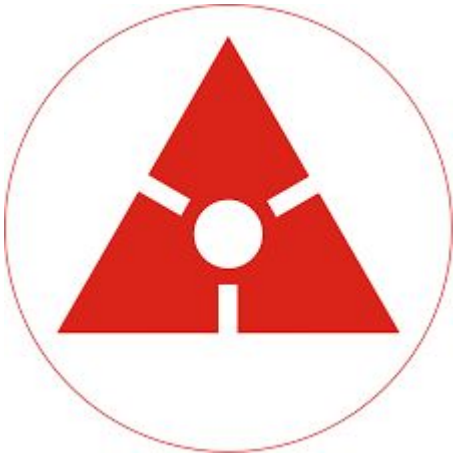
DDoS-атака типа HTTP Flood

Атака HTTP Flood осуществляется на уровне 7 модели OSI, который является уровнем приложений и на котором осуществляют работу протоколы HTTP, HTTPS, FTP и другие.



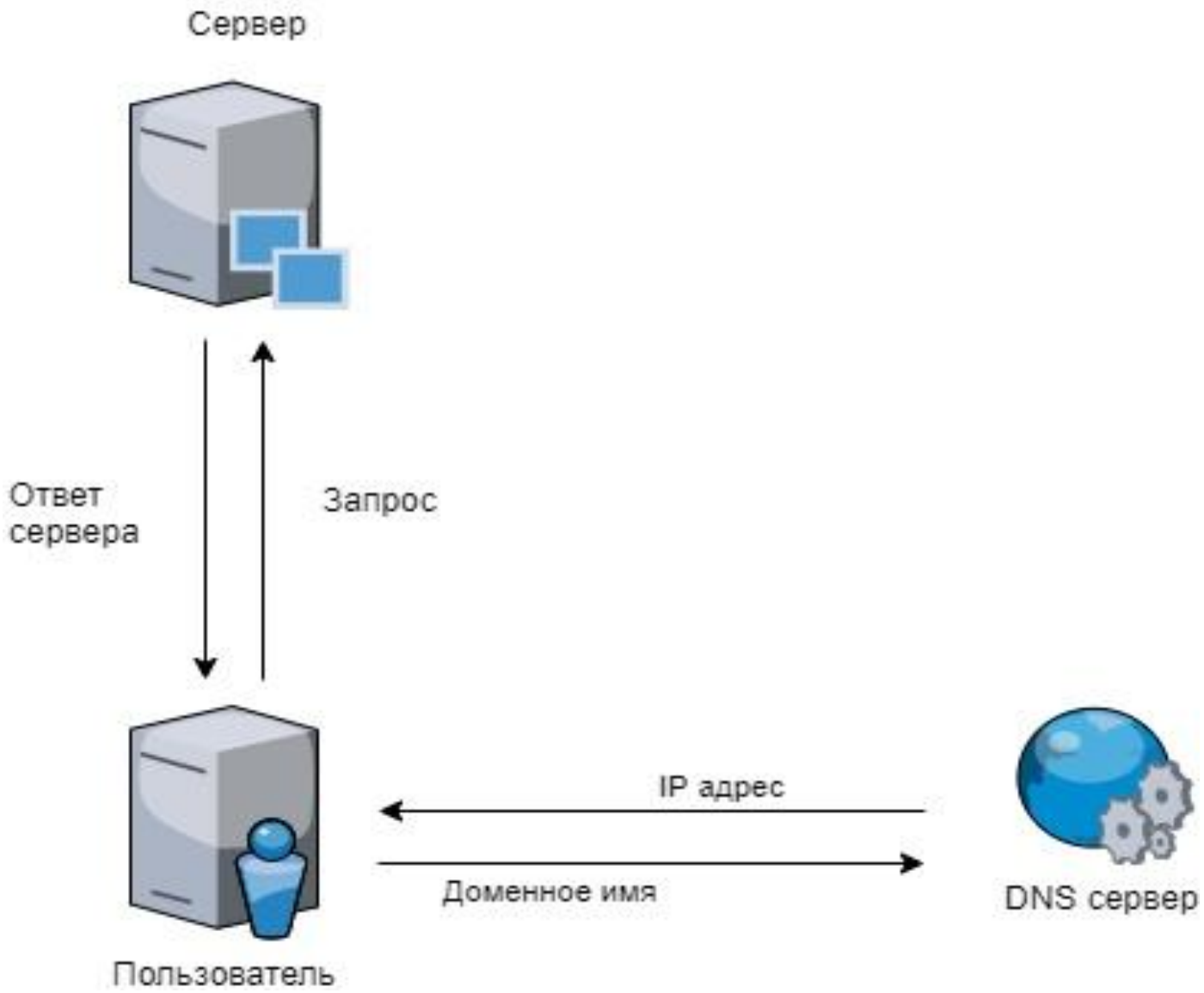
Представленные на рынке решения

Технология Cisco Clean PIPes предполагает использование модулей Cisco Anomaly Detector и Cisco Guard, а также различные системы статистического анализа сетевого трафика, основанные на данных, получаемых с маршрутизаторов по протоколу Cisco Netflow.



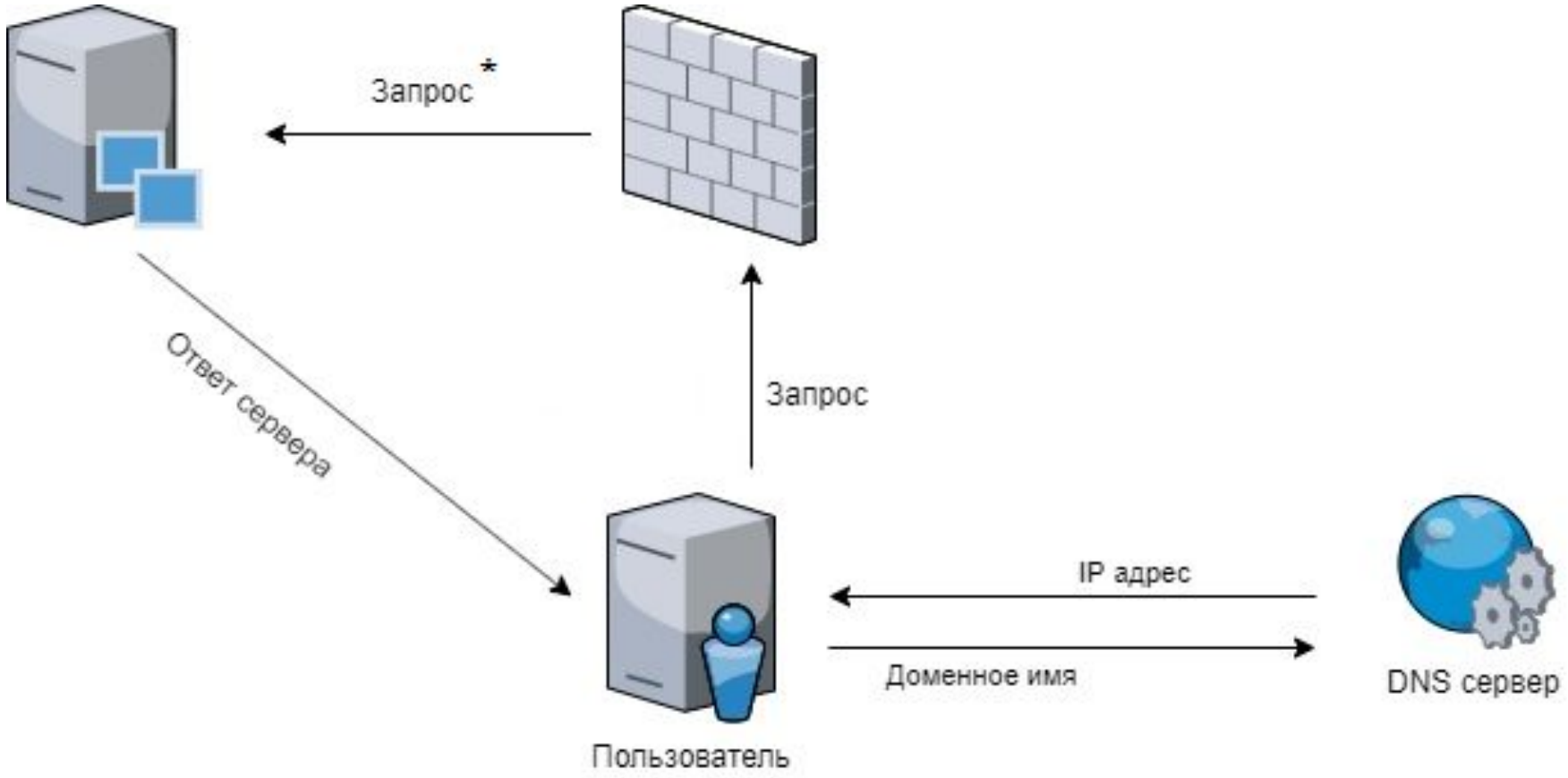
Модуль ados_daemon получает доступ к получаемым пакетам от HTTP-клиентов и принимает решение об их дальнейшей судьбе. В ходе работы производится сравнение IP-адреса источника с сформированными списками адресов.

Принцип отправки запросов в глобальной сети Интернет



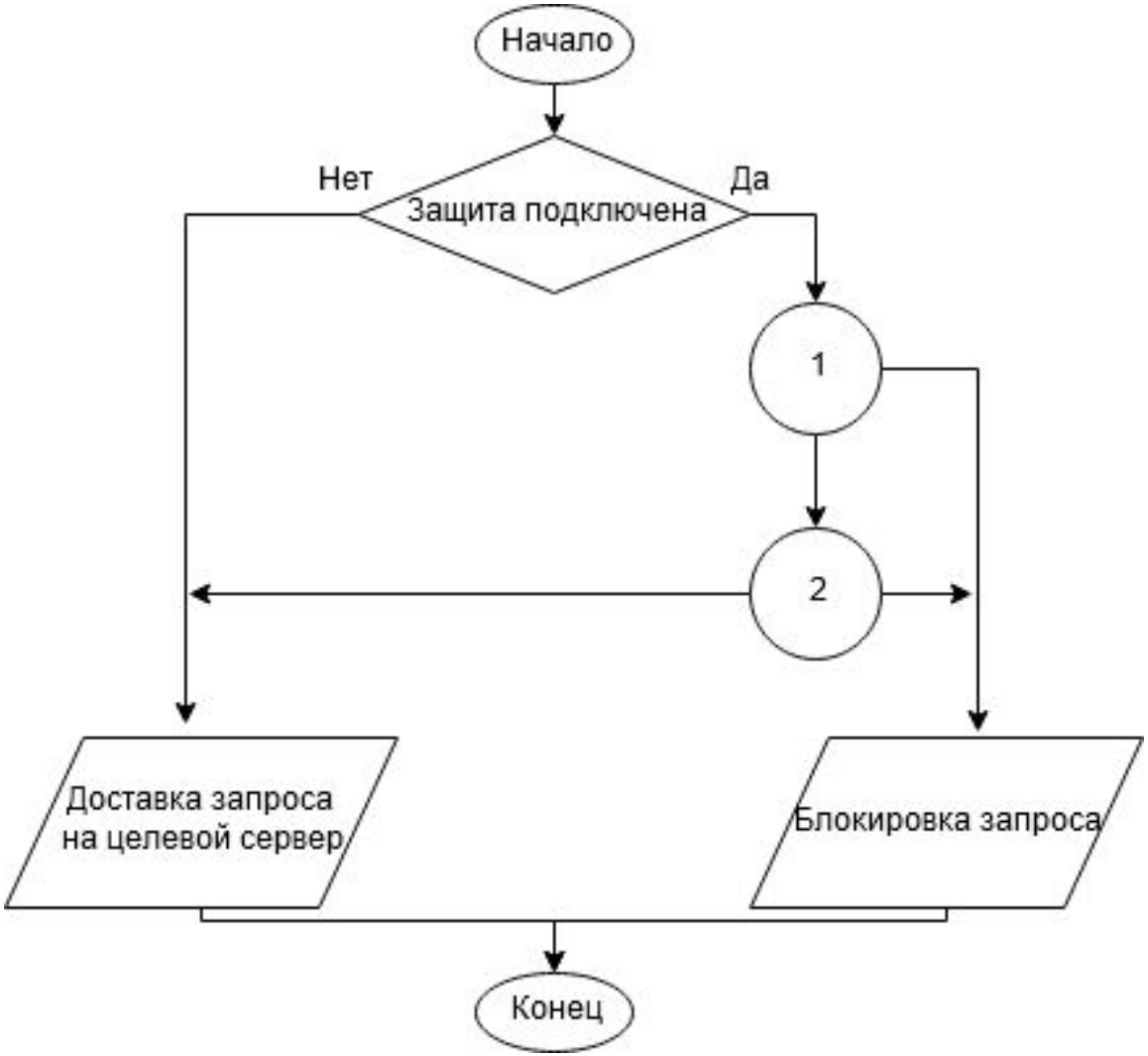
Предлагаемое решение

Предлагаемый принцип доставки запросов на целевой веб-сервер

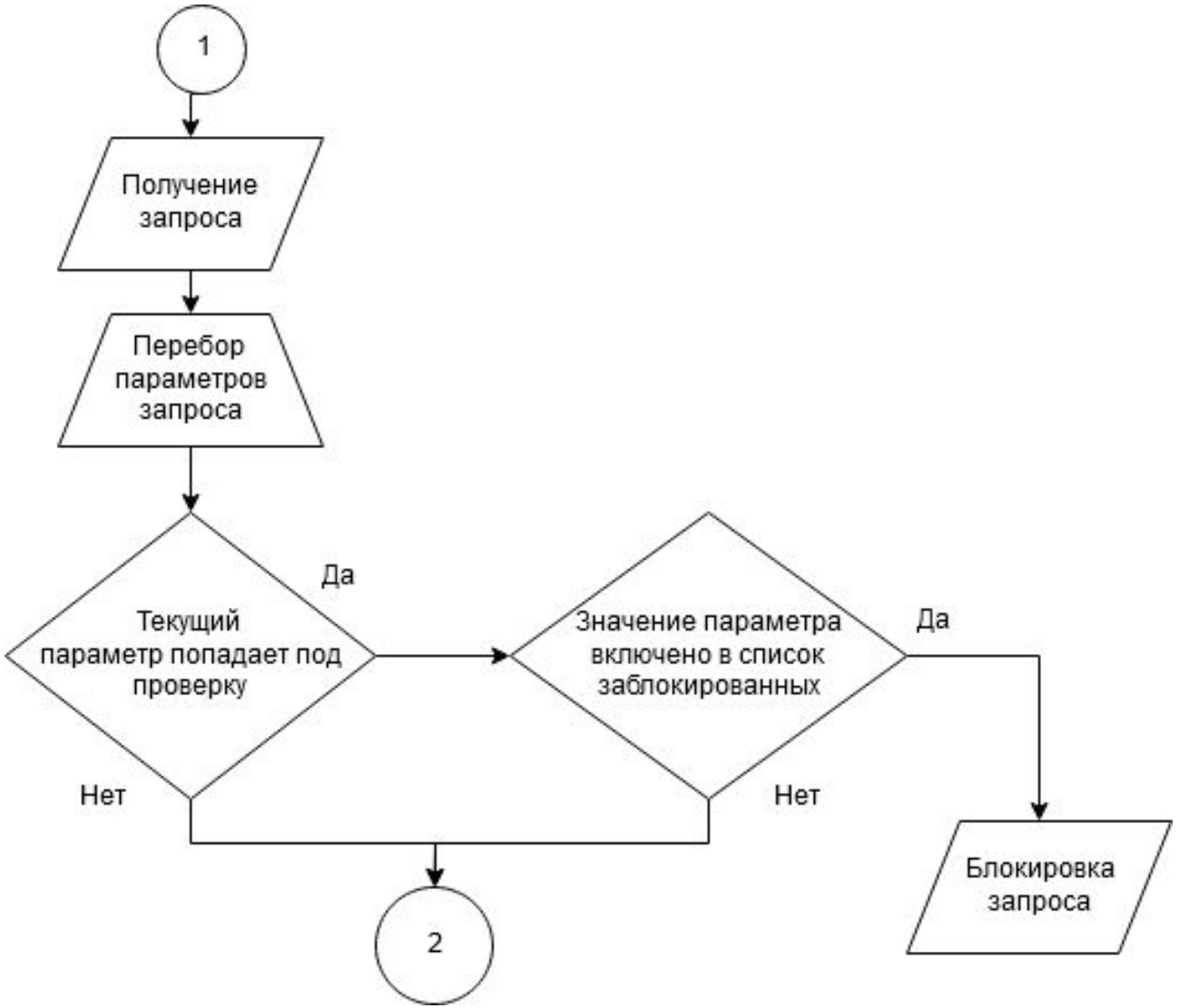


* Запросы от системы защиты на целевой сервер отправляются из ограниченного диапазона IP-адресов

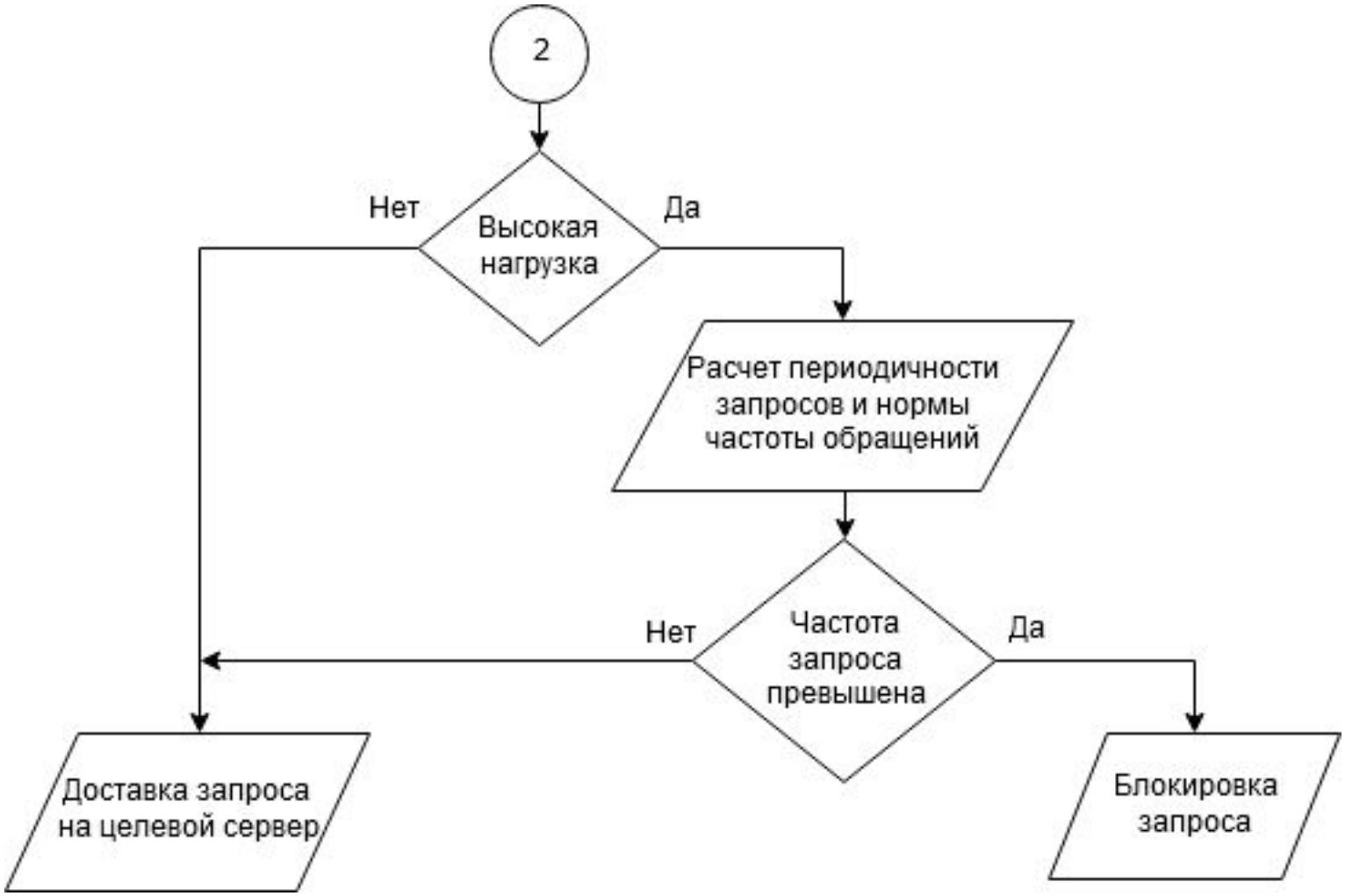
Аналитическая разработка системы отражения атак HTTP Flood



Аналитическая разработка системы отражения атак HTTP Flood



Аналитическая разработка системы отражения атак HTTP Flood



Особенности системы блокировки

Блокировка по тайм-ауту.

При нагрузке на сервер более 90% рассчитывается норма количества запросов:

$$q = \frac{C_1 * W_1 + \cdots + C_n * W_n}{t},$$

где C_i - количество запросов с IP-адреса за время t;

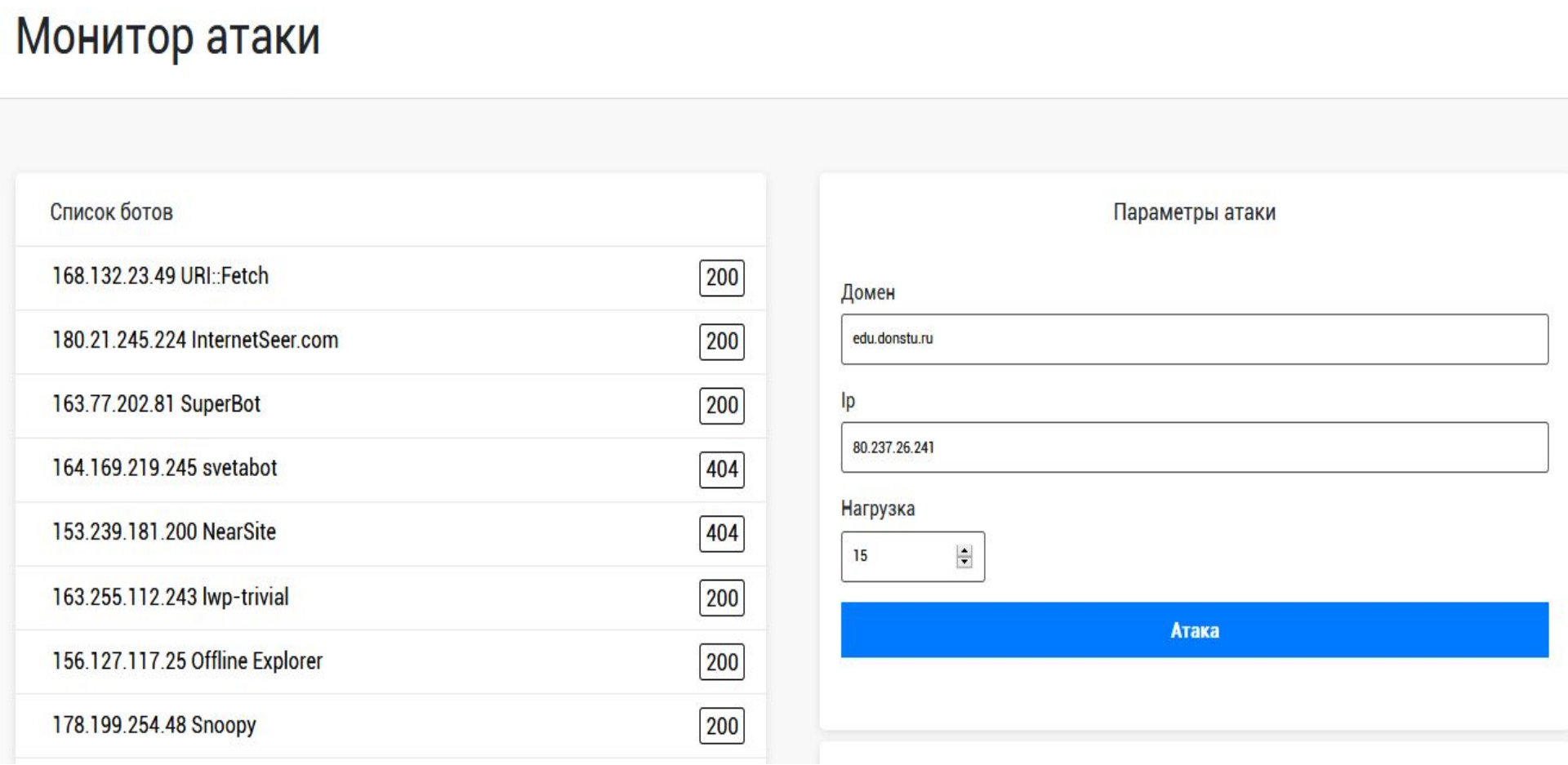
W_i - среднее время между запросами с IP-адреса за время t;

t – промежуток времен, в течение которого рассчитывается частота запросов.

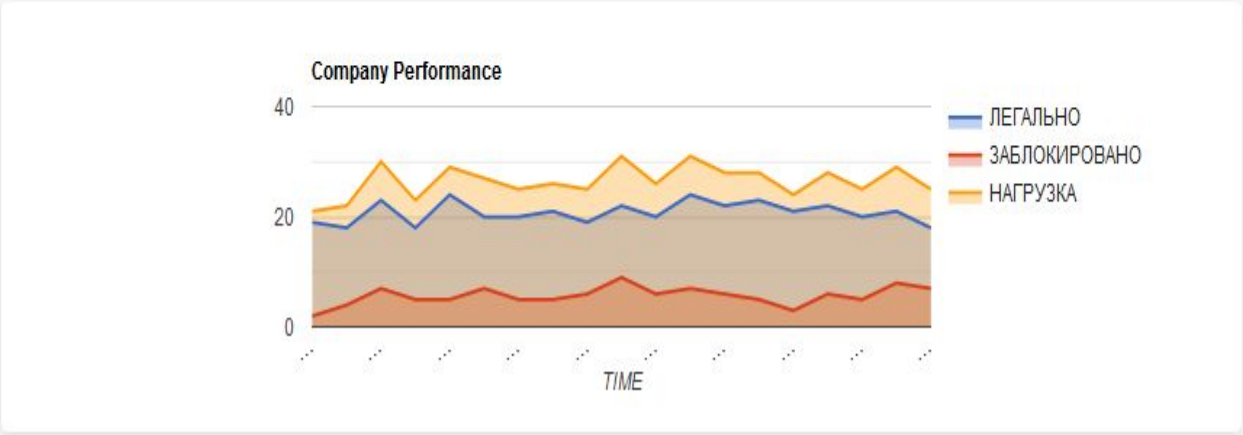
q – норма запросов в единицу времени t.

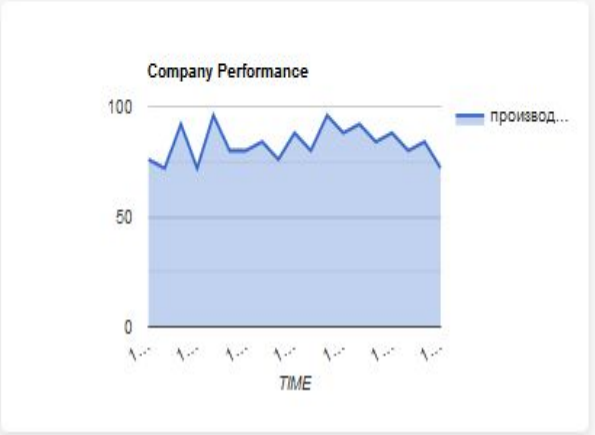
Если количество запросов в единицу времени t превышает норму на 75%, то IP-адрес источника запроса блокируется.

Демонстрационный режим



Монитор защиты





Нагрузка: **21** в секунду

156.127.117.25	80.237.26.241	GET	Offline Explorer	edu.donstu.ru	200
177.211.107.59	80.237.26.241	GET	LinksManager.com_bot	edu.donstu.ru	200
163.77.202.81	80.237.26.241	POST	SuperBot	edu.donstu.ru	200
152.250.167.151	80.237.26.241	POST	SearchmetricsBot	edu.donstu.ru	200
180.30.168.212	80.237.26.241	GET	Bot mailto:craftbot@yahoo.com	edu.donstu.ru	200
156.127.117.25	80.237.26.241	GET	Offline Explorer	edu.donstu.ru	200
168.132.23.49	80.237.26.241	POST	URI::Fetch	edu.donstu.ru	200
178.102.37.111	80.237.26.241	GET	CazoodleBot	edu.donstu.ru	404
161.67.158.210	80.237.26.241	POST	Grafula	edu.donstu.ru	404
180.30.168.212	80.237.26.241	GET	Bot mailto:craftbot@yahoo.com	edu.donstu.ru	200
180.21.245.224	80.237.26.241	POST	InternetSeer.com	edu.donstu.ru	200
177.211.107.59	80.237.26.241	POST	LinksManager.com_bot	edu.donstu.ru	200
180.105.69.52	80.237.26.241	POST	ExtractorPro	edu.donstu.ru	200
164.97.46.42	80.237.26.241	GET	ecxi	edu.donstu.ru	200
179.127.170.13	80.237.26.241	POST	Mozilla.*Indy	edu.donstu.ru	200
155.144.240.166	80.237.26.241	POST	Firefox/63	edu.donstu.ru	200
164.153.70.160	80.237.26.241	POST	Edge/16	edu.donstu.ru	200
170.11.191.63	80.237.26.241	GET	YandexBot	edu.donstu.ru	200
158.186.32.198	80.237.26.241	POST	SamsungBrowser/7	edu.donstu.ru	200

Внимание
Есть вероятность отключение сервера

Параметры фильтра

Добавить

agent	NearSite
ip	12
agent	WPScan
agent	IDBot
load	25
agent	CazoodleBot
agent	NearSite
agent	PECL::HTTP
agent	Web Sucker
agent	Express WebPictures
agent	sucker
agent	FlashGet

Заключение

Аналитически разработан алгоритм обнаружения и блокирования DDoS-атак типа HTTP Flood.

Разработано демонстрационное программное средство, основано на указанном принципе блокировки невалидных атакующих IP-адресов.

Реализовано 2 режима работы: с защитой и без защиты.

Проведены экспериментальные исследования алгоритма, в ходе которых была доказана эффективность разработанного алгоритма.

Список публикаций

1) Научная статья «Эллиптические кривые и методы их генерации» - Молодой исследователь Дона, 2018.
2) Научная статья «Повышение быстродействия квантового алгоритма факторизации П. Шора путём совершенствования его классической части» - Современные наукоемкие технологии. – 2019. – № 1 – С. 114-118.
3) Научная Статья «Сравнительный анализ легковесных блочных алгоритмов шифрования Nash и Speck, используемых в устройствах с ограниченными возможностями (микроконтроллерах)» - Молодой исследователь Дона, 2019.
4) Научная статья «Потенциальные угрозы безопасности данных, свя-занные с таргетированно-стью контента в информа-ционной сети интернет. Способы программной за-щиты устройств от вредо-носного программного обеспечения», Наука и инновации – современные концепции, 19 ап-реля 2019. – Москва.: 2019. С. 112-122.
5) Научная статья «Сравнительный анализ модифицированной постквантовой криптографической системы NTRUEncpypt с общепринятой криптосистемой RSA», Вестник Донского государственного технического университета. 2019. Т. 19, №2. С. 185-193.
6) Научная статья «Модернизация классической части квантового алгоритма П. Шора», Сборник трудов VIII Конгресса Молодых ученых, 15-19 апреля 2019 года. – СПб.: Университет ИТМО, 2019.
7) Научная статья «Преступная деятельность в интернете и способы борьбы с ней», Österreichisches Multiscience Journal. – 2019. - № 17. – Vol 1. - P. 54-58.
8) Научная статья «Незаконная деятельность в теневой паутине и способы борьбы с нею», «World Science - 2019» III международная научно-практическая конференция, Карловы Вары, Чехия, 29-30 мая 2019. – Москва., 2019. С 74-83.
9) Научная статья «Тестирование методов обмена данными между процессами на суперкомпьютере Jetson TX2 в сравнении с другими платформами», Сборник избранных статей по материалам научных конференций ГНИИ «Нацразвитие» (Санкт-Петербург, Июнь 2019). Международная научная конференция «Наука. Исследования. Практика». – СПб.: ГНИИ «Нацразвитие», 2019.
0) Научная статья «О безопасности интернета вещей», Сборник избран-ных статей по ма-териалам научных конференций ГНИИ «Нацразвитие» (Санкт-Петербург, Июнь 2019). Международная научная конференция «Безопасность: Информация, Техника, Управление». – СПб.: ГНИИ «Нацразвитие», 2019.

Спасибо за внимание