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:

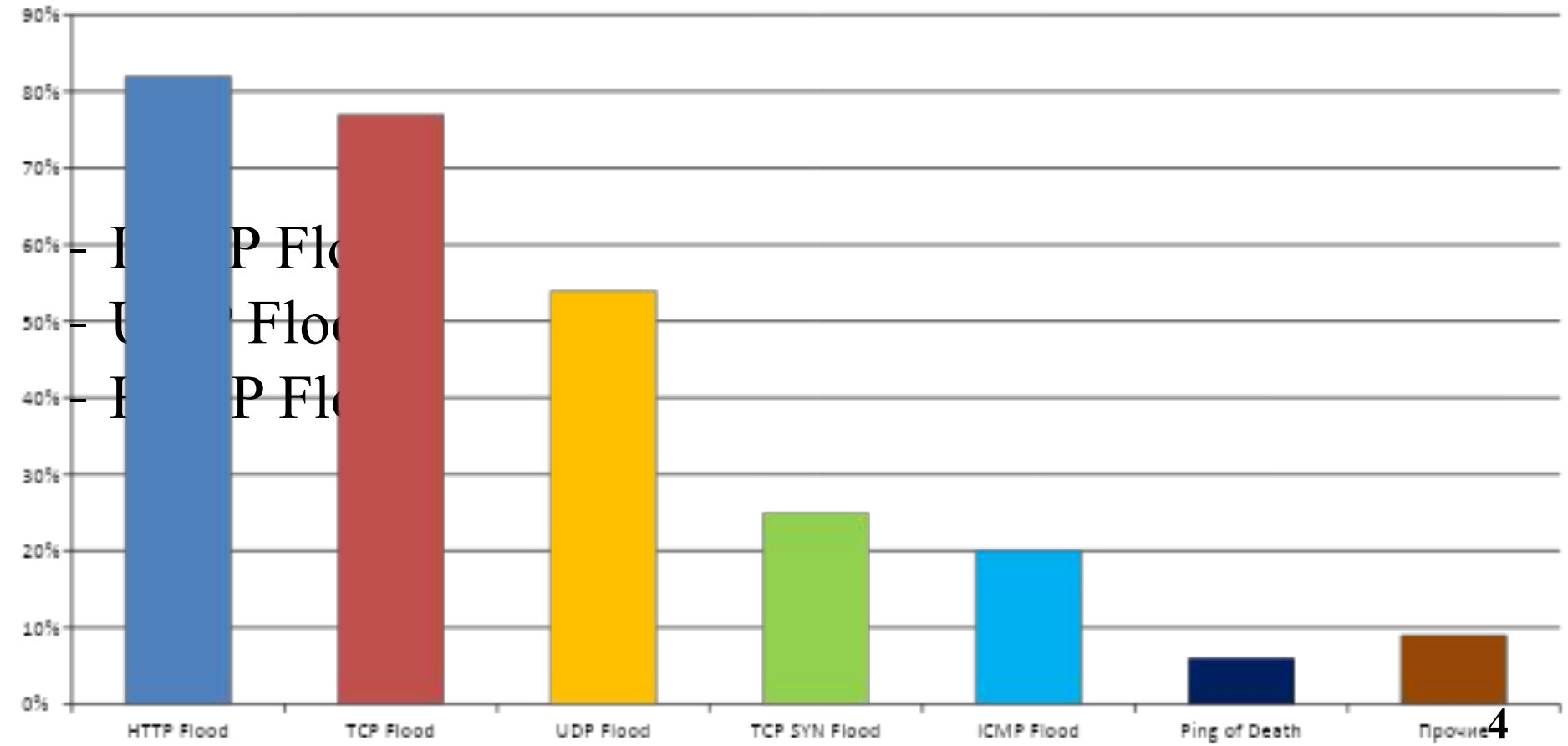
Защитный механизм противодействия DDoS-атакам HTTP Flood, совершаемым на уровне L7 модели OSI.

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.

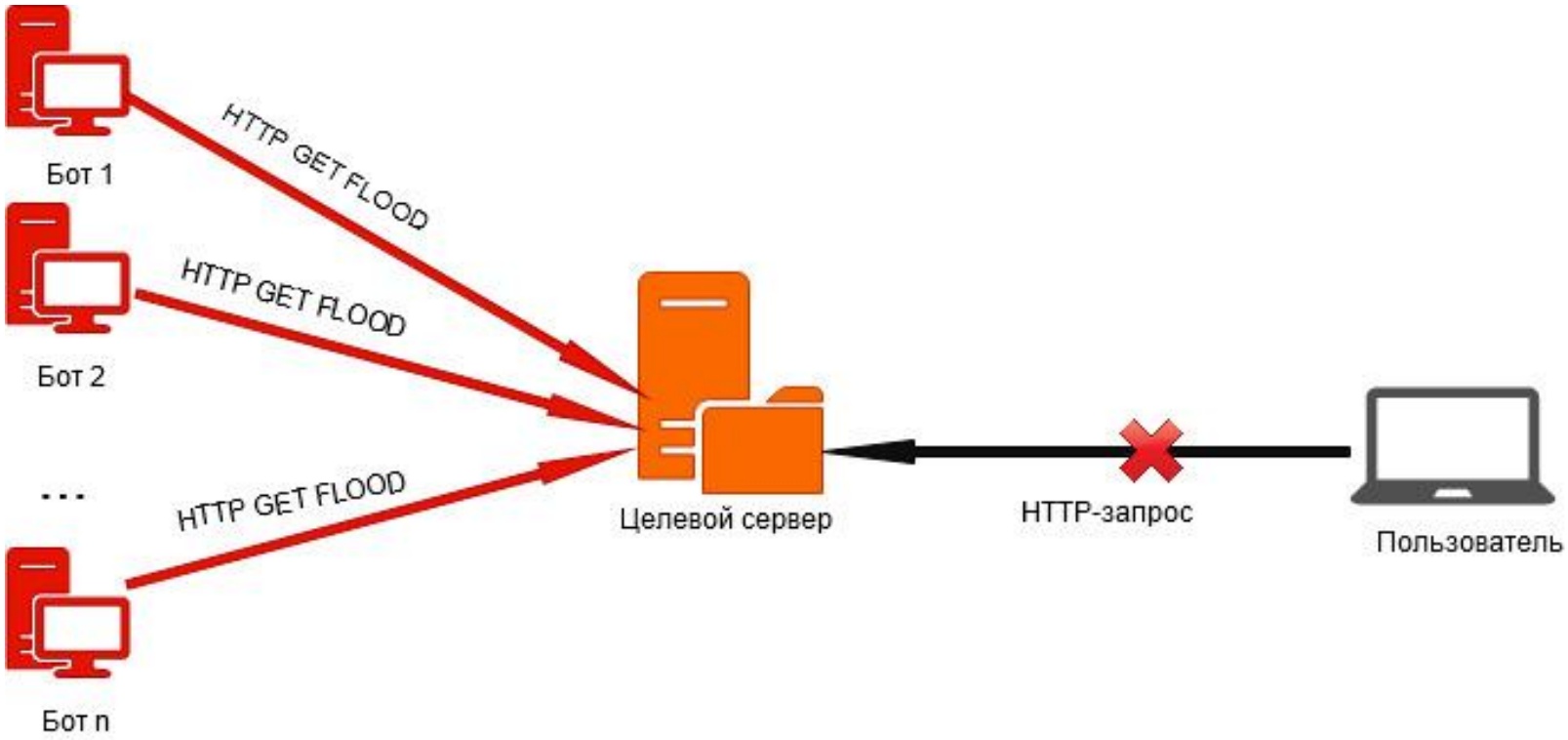
Наиболее распространенные DDoS-атаки

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



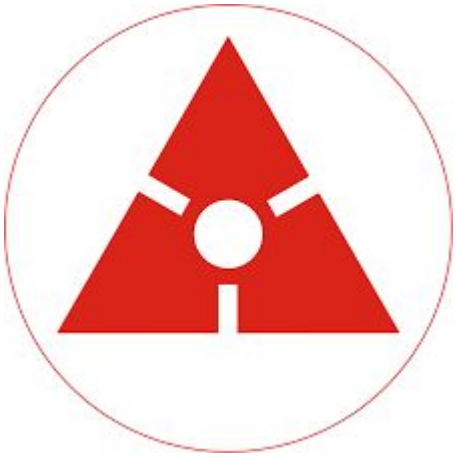
DDoS-атака типа HTTP Flood

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



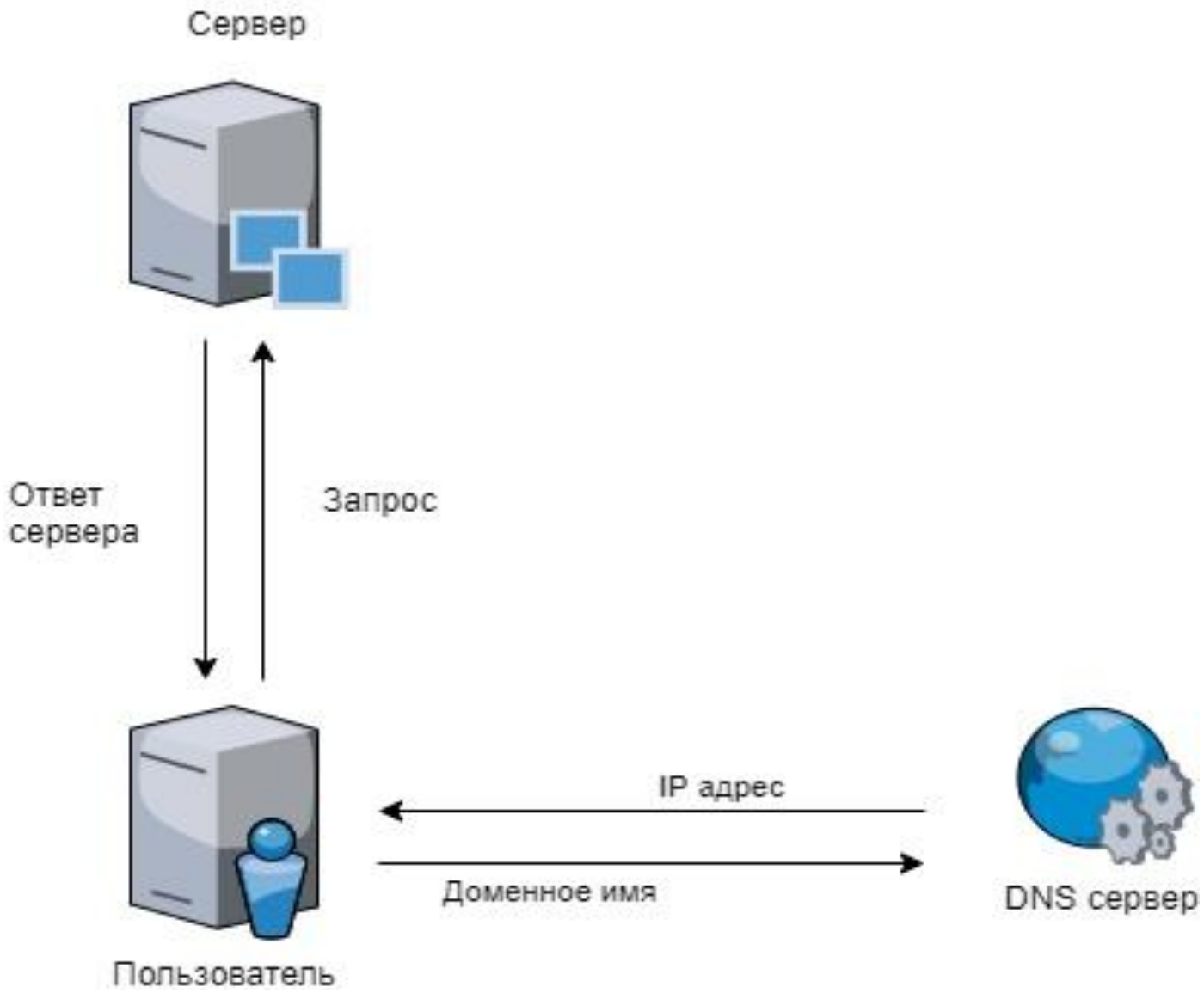
Представленные на рынке решения

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.



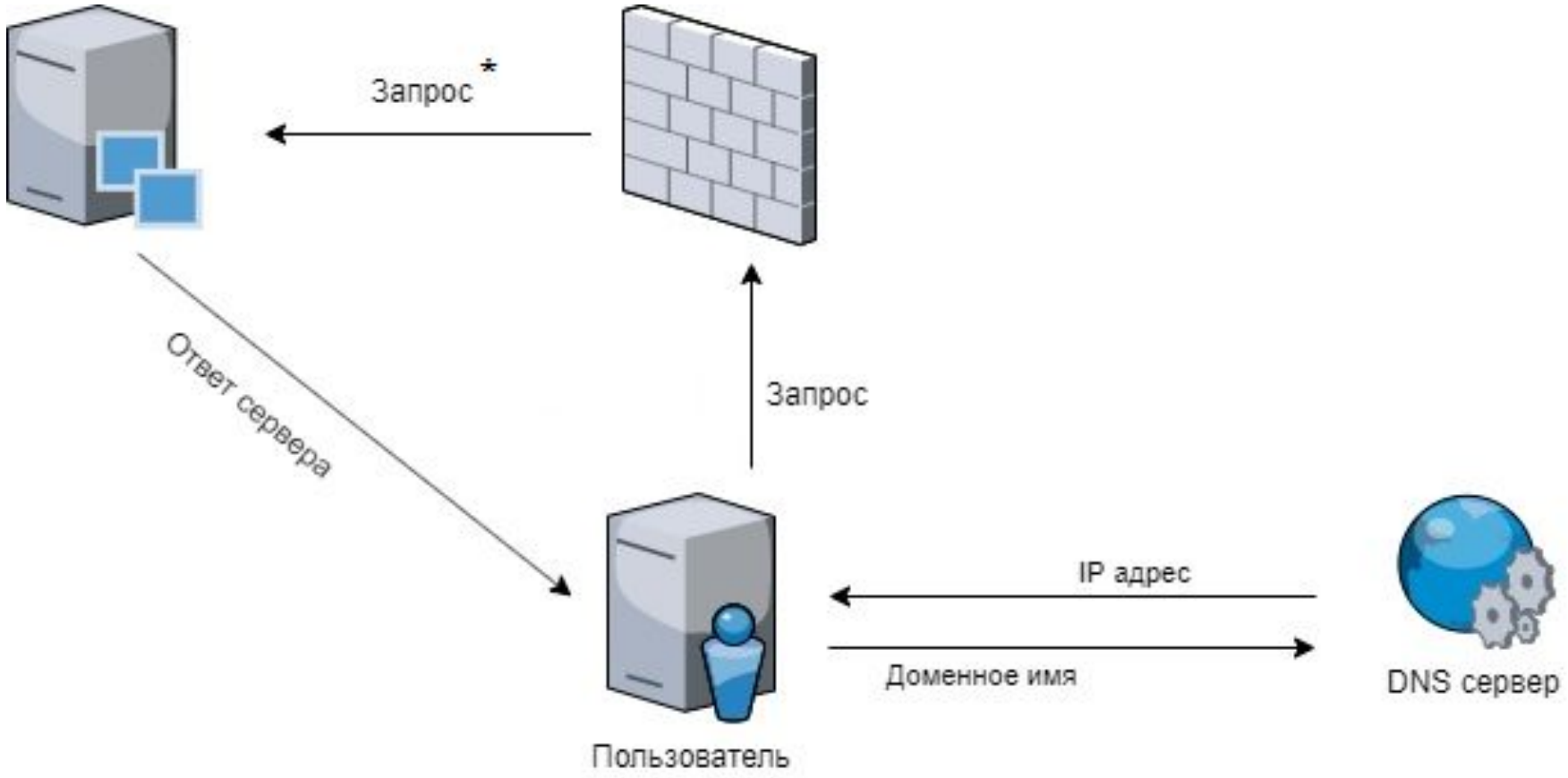
Модуль ados_daemon получает доступ к получаемым пакетам от HTTP-клиентов и принимает решение об их дальнейшей судьбе. В ходе работы производится сравнение IP-адреса источника с сформированными списками адресов.

Принцип отправки запросов в глобальной сети Интернет



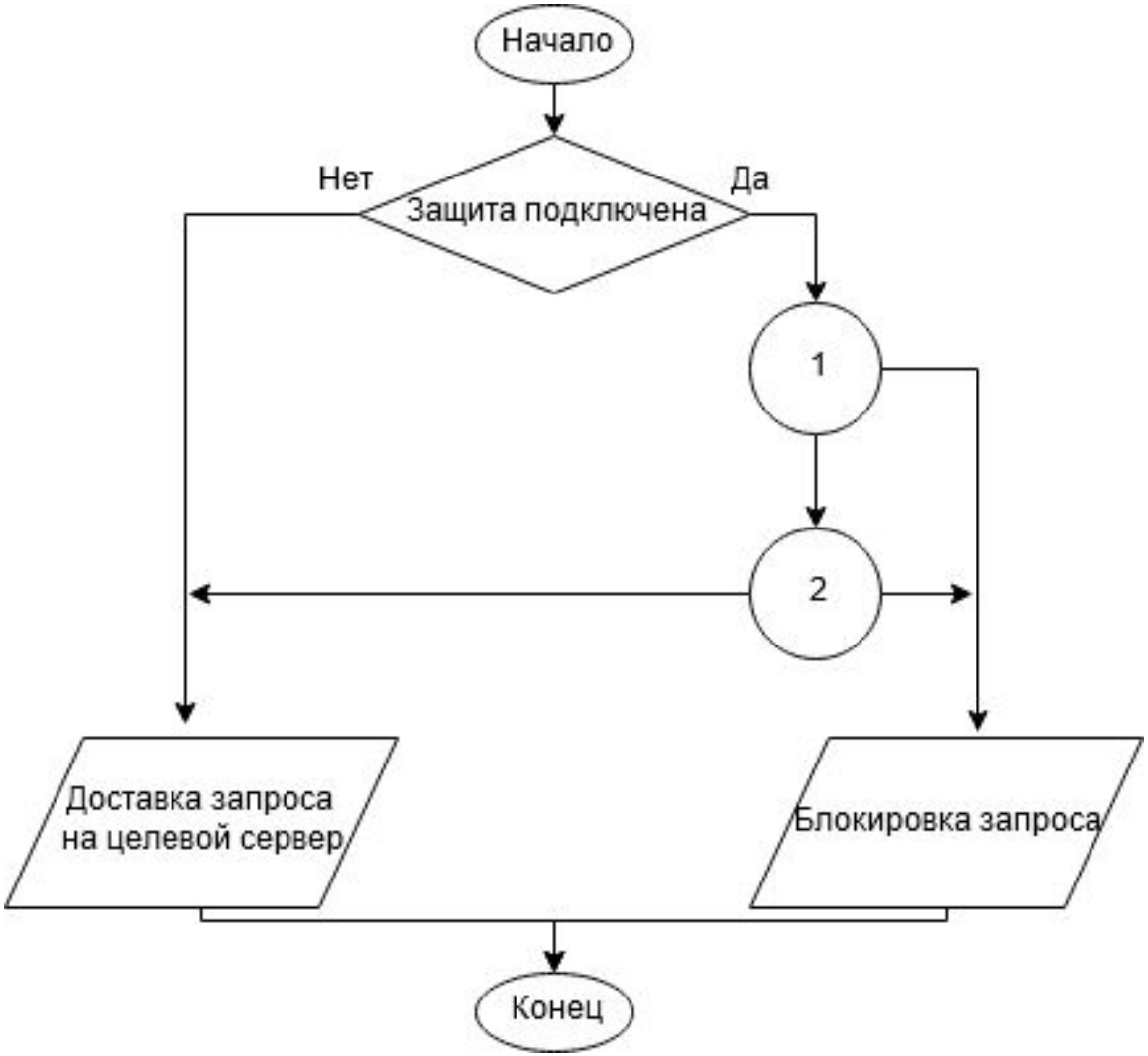
Предлагаемое решение

Предлагаемый принцип доставки запросов на целевой веб-сервер

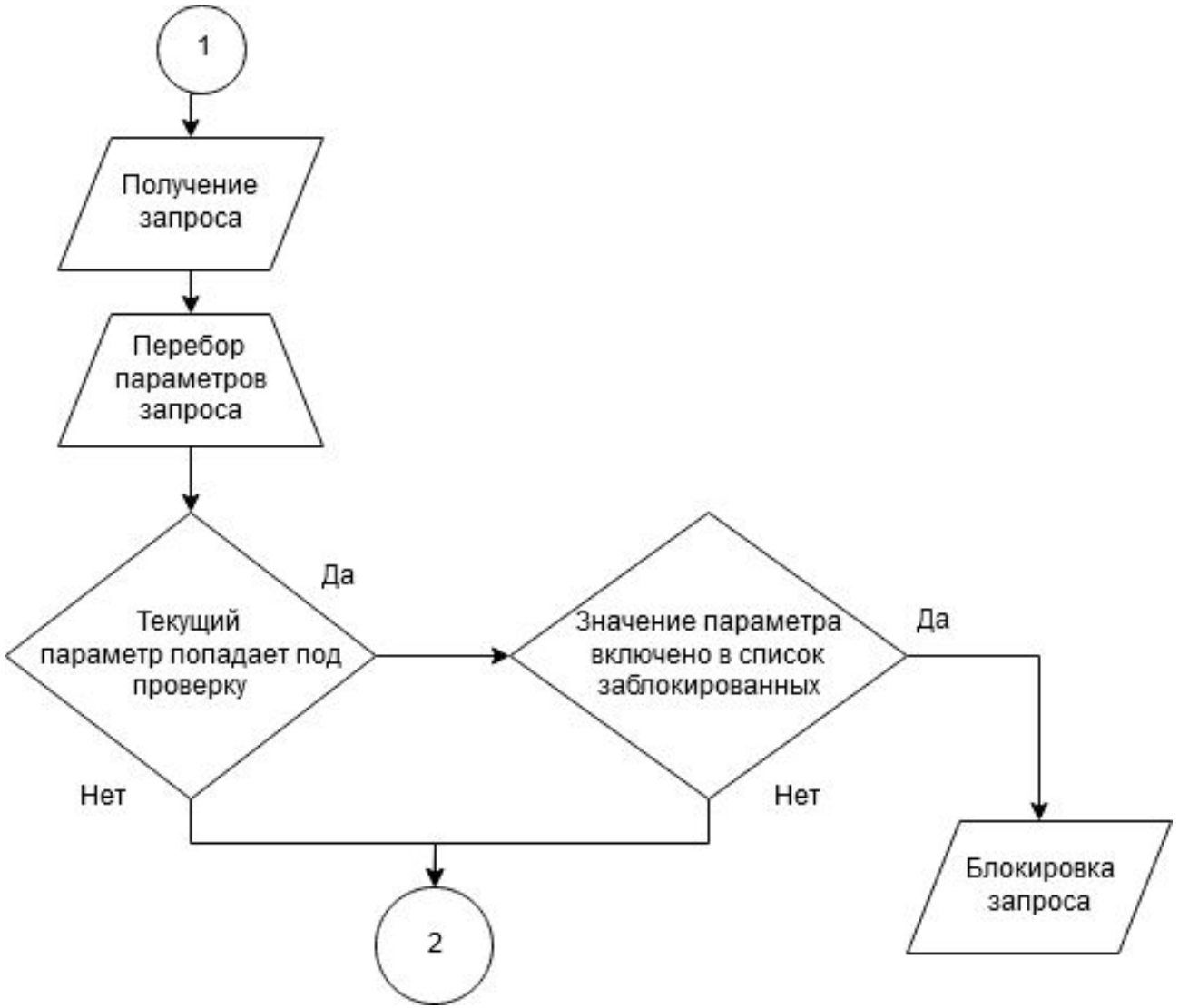


* Запросы от системы защиты на целевой сервер отправляются из ограниченного диапазона IP-адресов

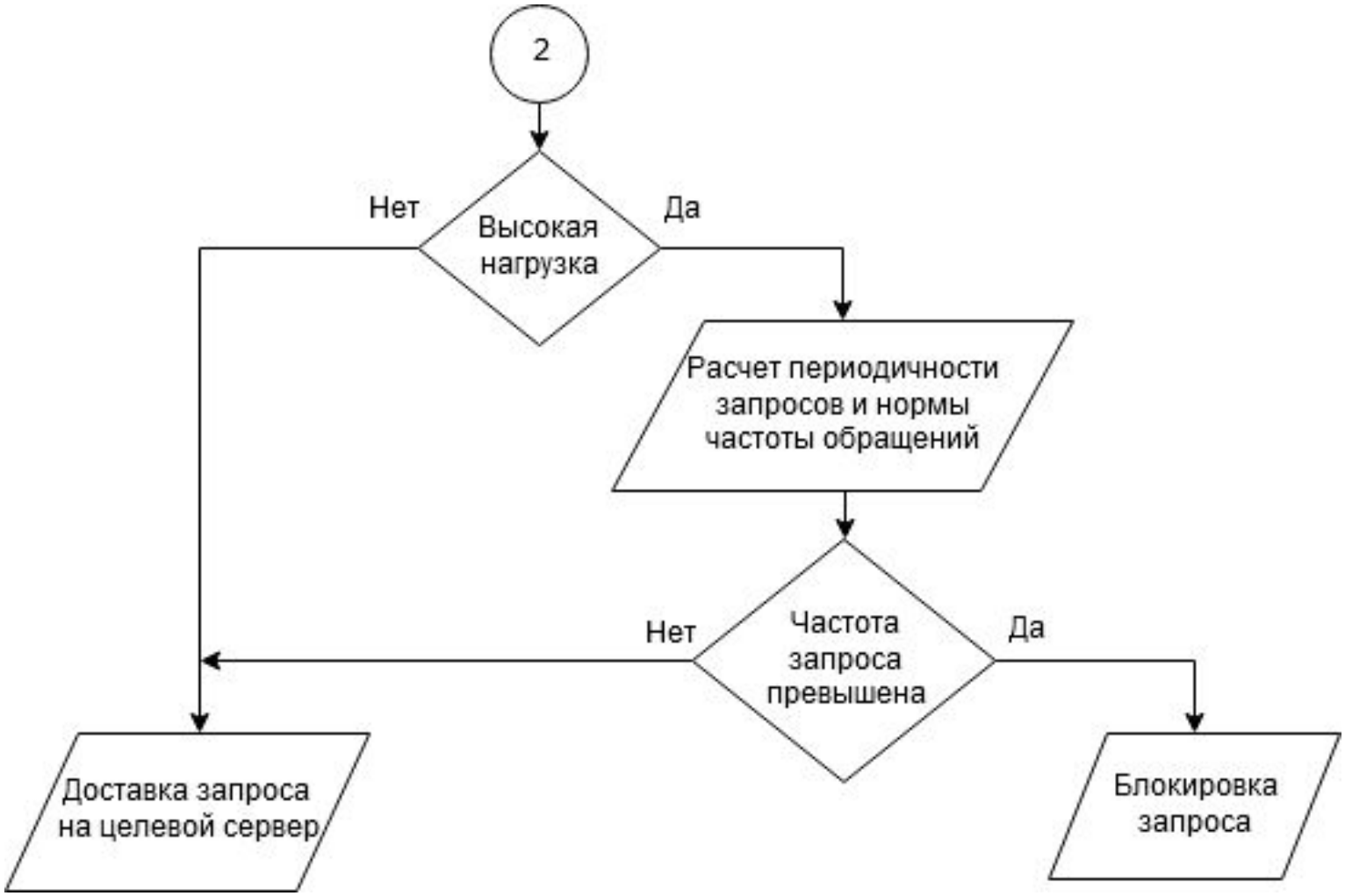
Аналитическая разработка системы отражения атак HTTP Flood



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;

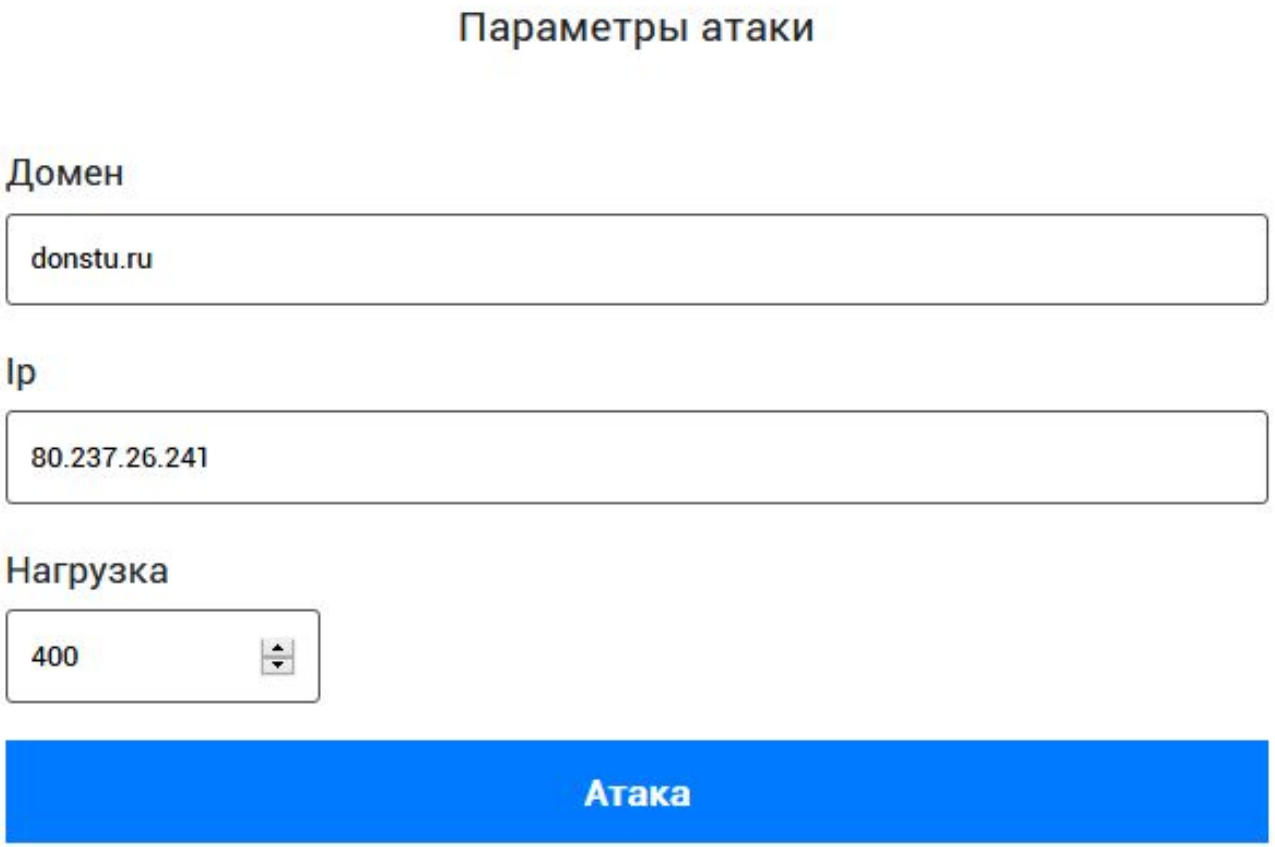
W_i - среднее время между запросами с IP-адреса за время t;

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



Демонстрационный режим

Список ботов

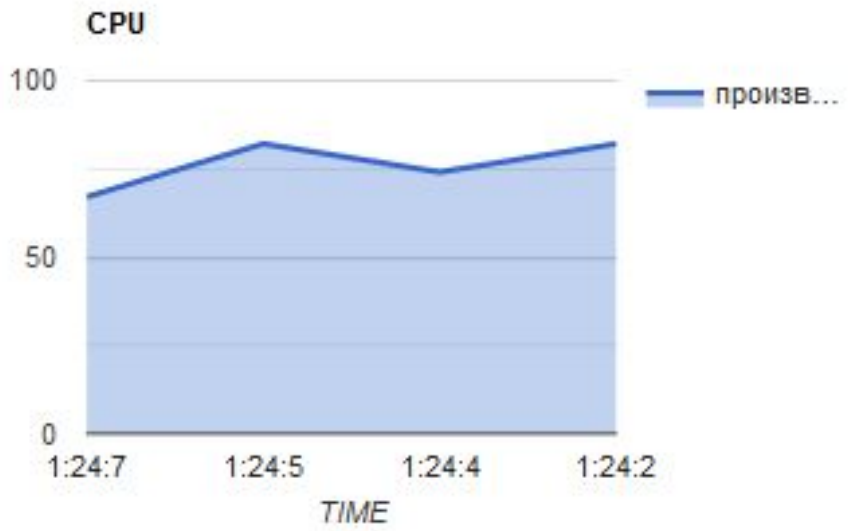
168.132.23.49 URI::Fetch	200
180.21.245.224 InternetSeer.com	200
163.77.202.81 SuperBot	200
164.169.219.245 svetabot	no response
153.239.181.200 NearSite	no response
163.255.112.243 lwp-trivial	200

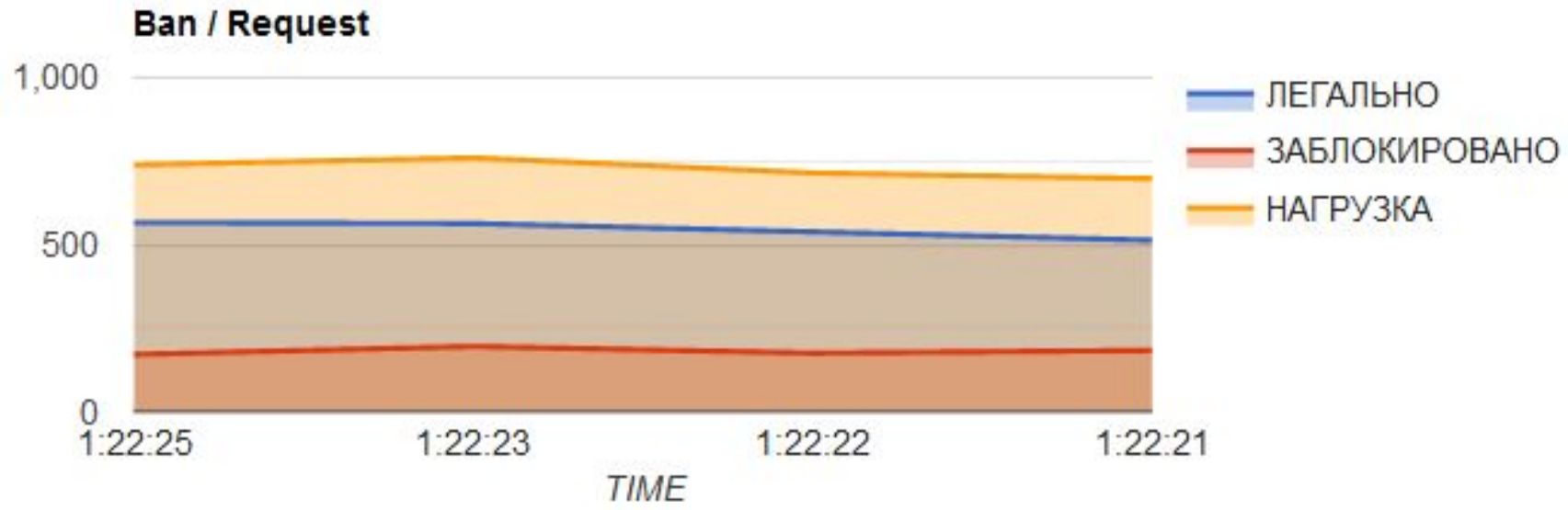
Монитор защиты

Параметры фильтра

Добавить

agent	NearSite
ip	12
agent	WPScan
agent	IDBot





Монитор защиты

Нагрузка: **374** в секунду

168.80.141.203	80.237.26.241	GET	sucker	donstu.ru	blocked	1:28:6
172.111.251.102	80.237.26.241	POST	SuperHTTP	donstu.ru	blocked	1:28:6
176.141.189.48	80.237.26.241	GET	Grafula	donstu.ru	blocked	1:28:6
180.105.69.52	80.237.26.241	GET	ExtractorPro	donstu.ru	200	1:28:6
153.68.232.86	80.237.26.241	GET	CazoodleBot	donstu.ru	blocked	1:28:6
179.98.175.22	80.237.26.241	GET	WPScan	donstu.ru	blocked	1:28:6
156.127.117.25	80.237.26.241	GET	Offline Explorer	donstu.ru	200	1:28:6
163.77.202.81	80.237.26.241	POST	SuperBot	donstu.ru	200	1:28:6
177.166.181.52	80.237.26.241	POST	libwww	donstu.ru	200	1:28:6
178.199.254.48	80.237.26.241	POST	Snoopy	donstu.ru	200	1:28:6
176.141.189.48	80.237.26.241	GET	Grafula	donstu.ru	blocked	1:28:6

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.

Проведены экспериментальные исследования алгоритма, в ходе которых была доказана эффективность разработанного алгоритма, при которой обеспечивается функционирование целевого сервера, а следовательно, и информационной системы, расположенной на нем.

Список публикаций

Scopus, Web of Science

1) Eliptic curves and methods of its generation. Actual problems of information technologies, electronics and radio engineering, 2018.

2) Modification and optimization of Pollard's factorization q-method by means of recursive algorithm of number calculation factorization. IEEE EWDTS 2019.

ВАК

1) Повышение быстродействия квантового алгоритма факторизации П. Шора путём усовершенствования его классической части. Современные наукоемкие технологии, 2019.

2) Сравнительный анализ модифицированной постквантовой криптографической системы NTRUEncrypt с общепринятой криптосистемой RSA. Вестник ДГТУ, 2019.

Прочие

1) Научная Статья «Сравнительный анализ легковесных блочных алгоритмов шифрования Nash и Speck, используемых в устройствах с ограниченными возможностями (микроконтроллерах)» - Молодой исследователь Дона, 2019.

2) Научная Статья «Сравнительный анализ легковесных блочных алгоритмов шифрования Nash и Speck, используемых в устройствах с ограниченными возможностями (микроконтроллерах)» - Молодой исследователь Дона, 2019.

Отправлены в печать

1) Разработка и анализ эффективности средств противодействия от DDoS-атак. Современные наукоемкие технологии.

Спасибо за внимание!