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

Программное средство обнаружения и противодействия импульсно-волновым DDoS-атакам (Pulse Wave)

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

Выполнил
студент группы ВКБ62
Ляшенко Кирилл
Александрович

2023

Объект исследования: информационные ресурсы, подверженные DDoS–атакам импульсно-волнового типа, с организацией серии коротких, но мощных импульсов атакующего трафика с определённой периодичностью.

Предмет исследования: алгоритм обнаружения и противодействия DDoS-атакам импульсно-волнового типа (Pulse-wave).

Цель работы: разработка алгоритма и программного средства обнаружения и противодействия DDoS-атакам импульсно-волнового типа.

Задачи исследования:

–классификация и изучение возможных типов DDoS-атак;

–анализ особенностей реализации DDoS-атак импульсно-волнового типа;

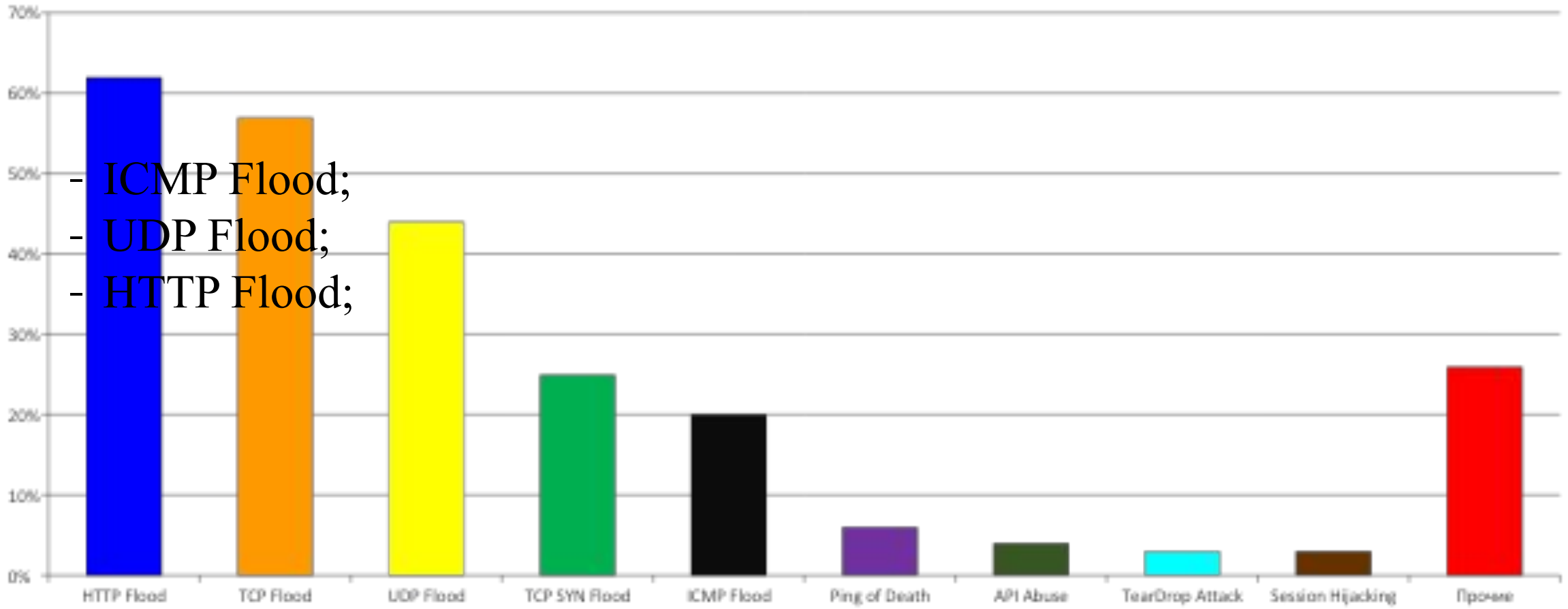
–разработка алгоритма обнаружения и противодействия DDoS-атаки типа Pulse-wave;

–создание программного приложения детектирования и нейтрализации DDoS-атак импульсно-волнового типа на языке программирования Python 3.9 в среде Pycharm;

–тестирование серверного оборудования, подверженного DDoS-атакам типа Pulse-wave, с целью проверки работы программного средства по созданию превентивных мер защиты.

Наиболее распространенные типы DDoS-атак

- TCP SYN Flood;
- TCP Flood;
- Ping of Death;
- ICMP Flood;
- UDP Flood;
- HTTP Flood;
- API Abuse;
- TearDrop Attack;
- Session Hijacking

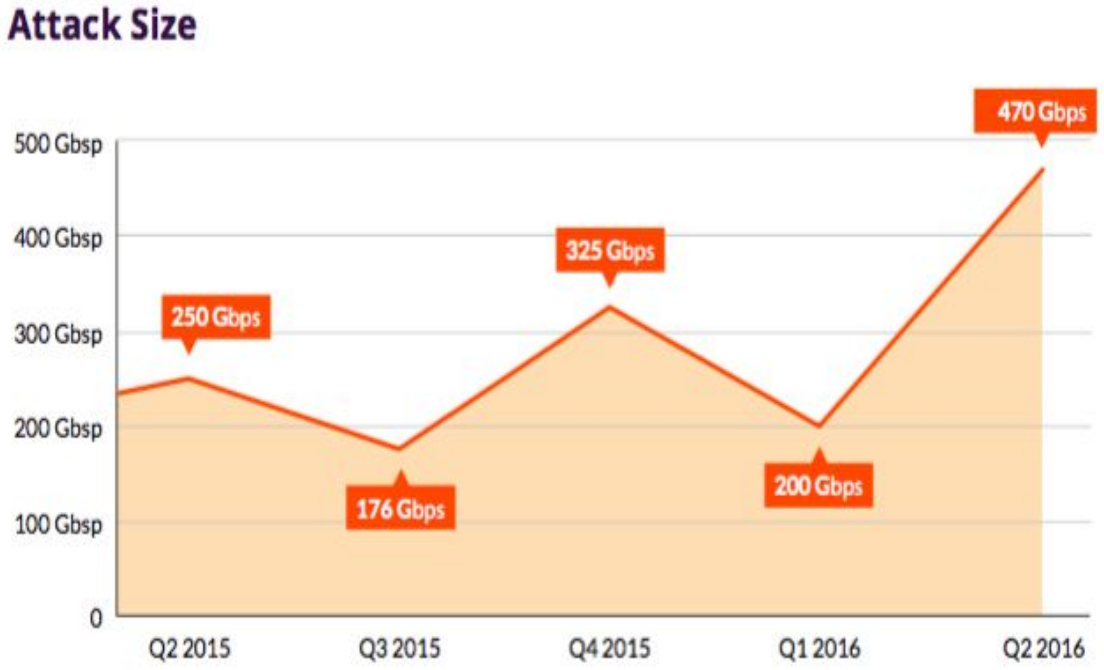


Жертвы DDoS-атак

Первое обнаружение импульсно-волновой DDoS-атаки

Во 2-м квартале 2016 г. В исследованиях компании Imperva была зарегистрирована атака объемом 470 Gbps, одна из крупнейших за историю Интернета.

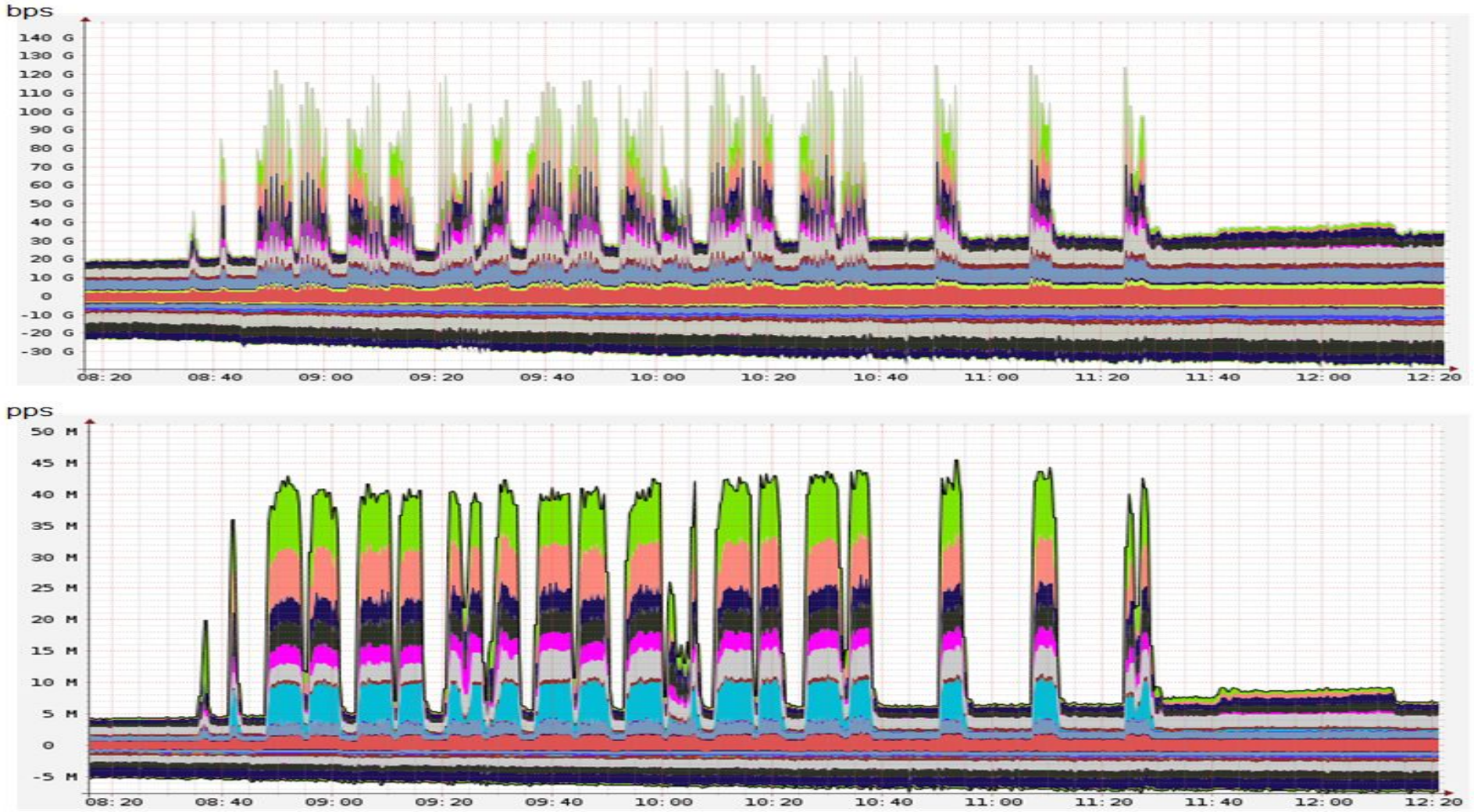
В первых числах марта 2018 года на GitHub обрушилась DDoS-атака, установившая новый рекорд: 1,35 Тб/сек или 126,9 млн пакетов в секунду. А уже 5 марта 2018 года была обнаружена DDoS-атака на американский сервис-провайдера, мощность составила 1,7 Тб/сек. Это новый рекорд и вновь «самая мощная DDoS-атака в истории».



https://www.imperva.com/blog/?category=network-security

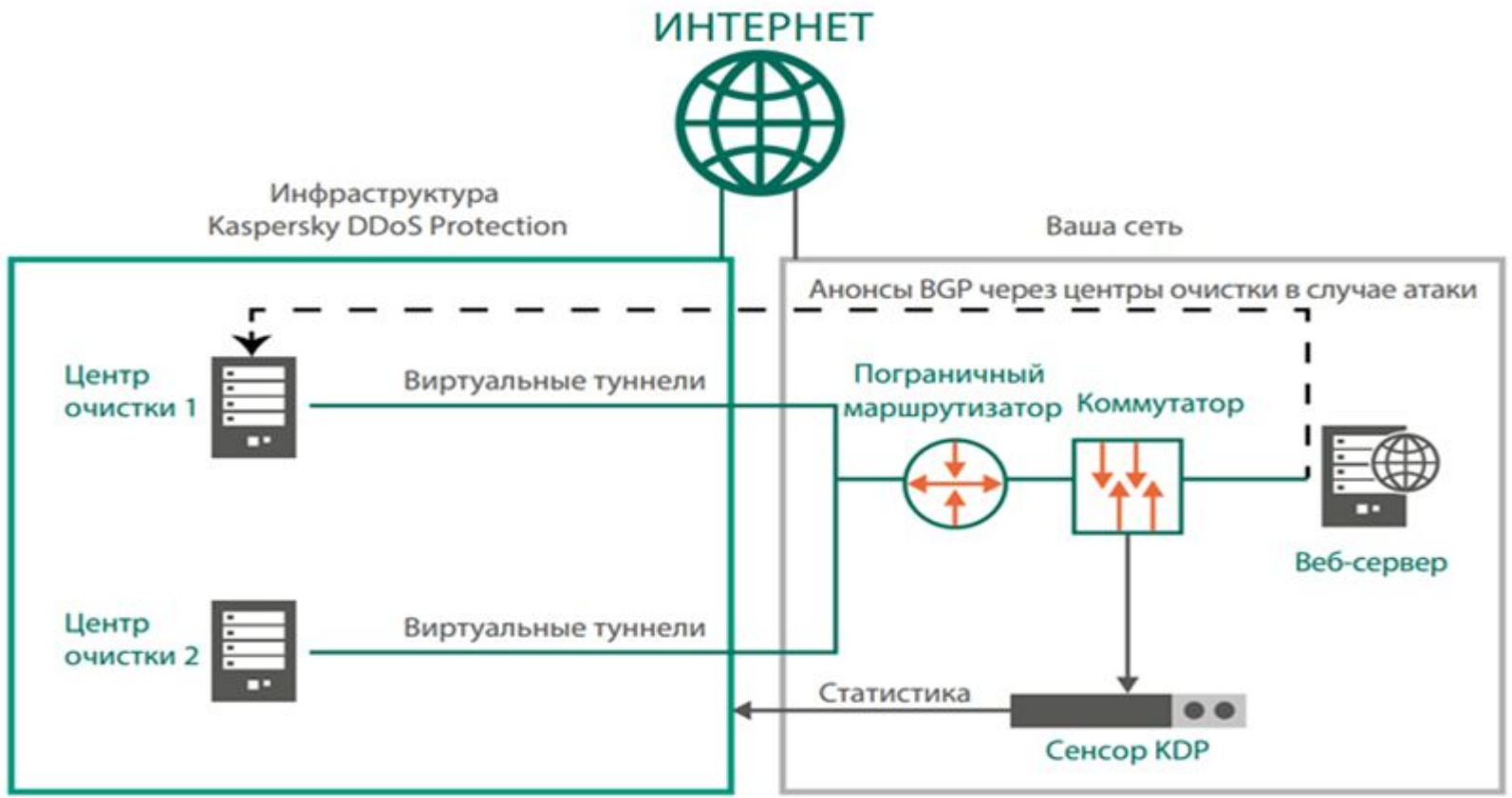
Действия злоумышленника при осуществлении импульсно-волновой DDoS-атаки

Атаки типа Pulse Wave чаще всего осуществляется на уровне 7 модели OSI, на котором осуществляют работу протоколы HTTP, HTTPS, FTP и др., хотя, кроме 7-го уровня, атака может использовать 3 и 4 уровни



Ранее предлагаемые технические решения

Большинство систем защиты от DDoS работают по схеме «анализ — обнаружение — переключение — очистка». Обнаружив аномалию, они меняют маршруты и перенаправляют трафик. Но с момента начала атаки и до момента пропуска трафика через устройство очистки ресурс остается незащищенным и, как правило, недоступным. Это является конечной целью злоумышленника.



АРХИТЕКТУРА KASPERSKY DDOS PROTECTION

Qrator — один из наиболее известных российских ресурсов по борьбе с DDoS. При отражения атаки на (7 уровене модели OSI) не требуется тонкой настройки продукта, при обнаружении атаки система перейдет в нужный режим автоматически

DDoS-Guard Protection — сервис защиты от ddos-атак, а также система фильтрации и шифрования трафика

Kaspersky DDoS Prevention

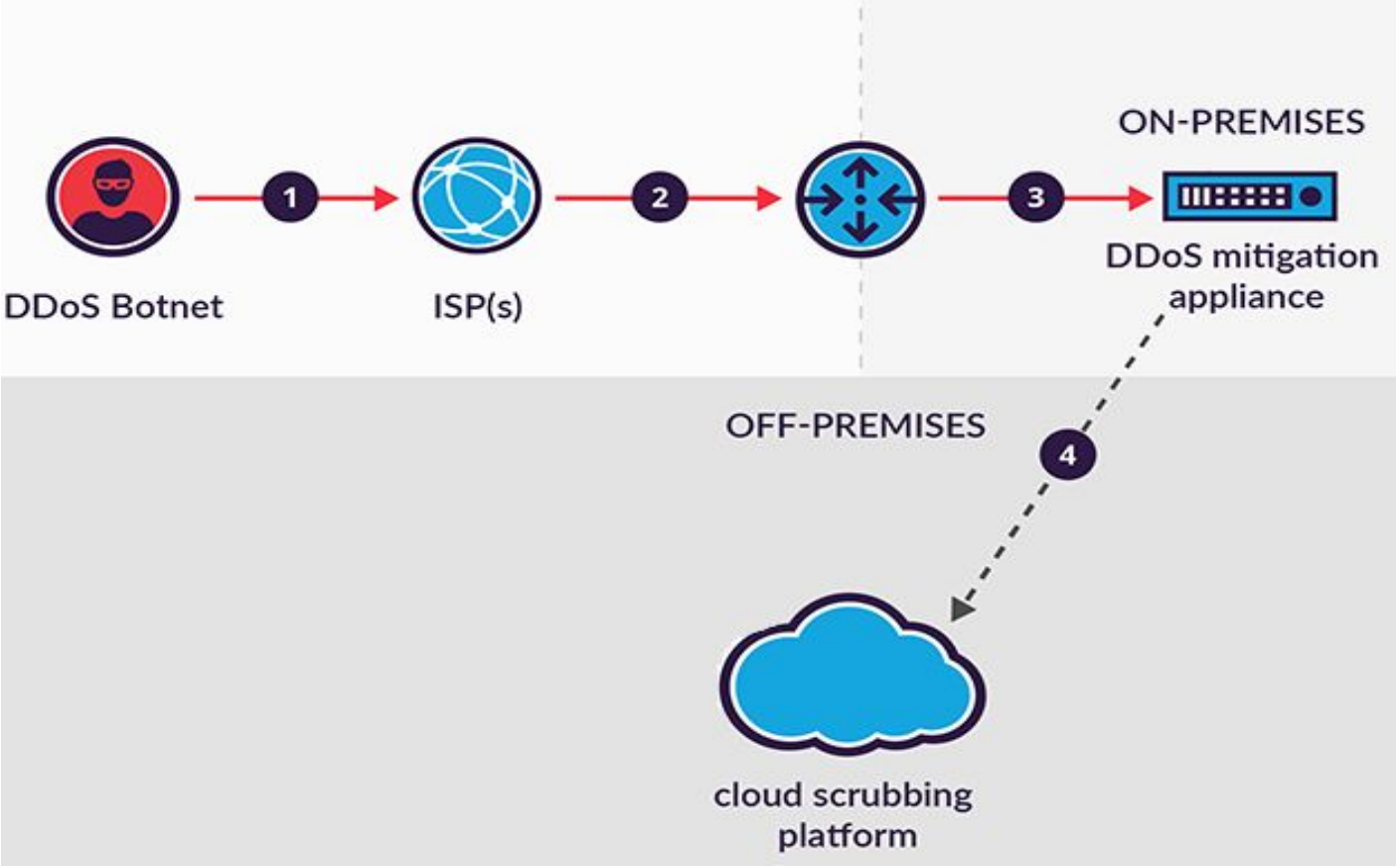
invGUARD

Гибридные решения проблемы противодействия импульсно-волновой DDoS-атаки

Гибридное решение — это решение задействовать облачный сервис anti-DDoS, который подключается автоматически при начале атаки. Гибридный подход позволяет устранить ограничения по объемам атак и воспользоваться разгрузкой и фильтрации трафика по средствам дополнительных вычислительных мощностей

Недостатки

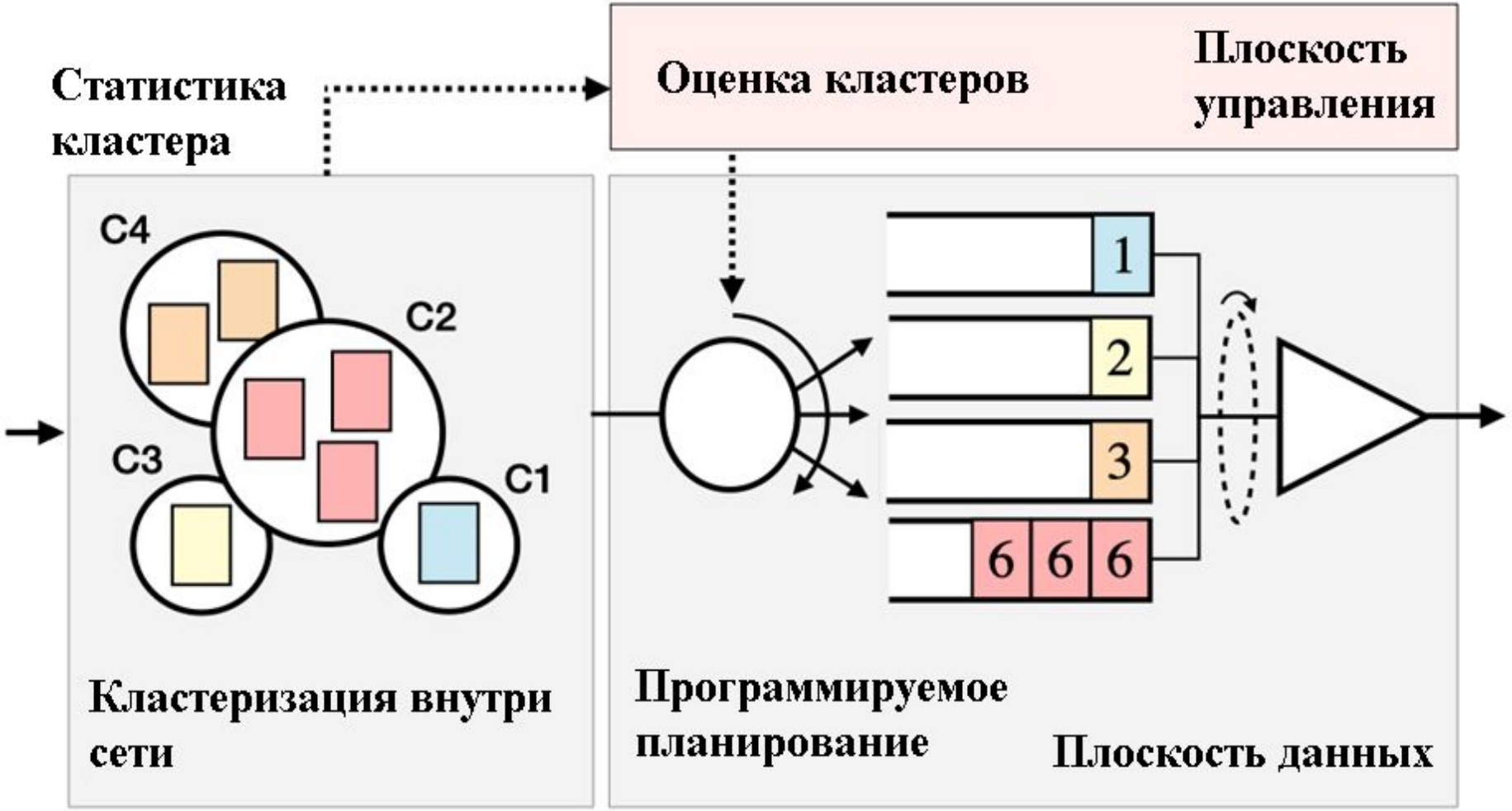
- увеличение задержки (трафик идёт сначала в центр очистки, затем к клиенту);
- необходимость пропуска конфиденциальных данных через облако;
- полностью арендованное решение, нет полноценного контроля.



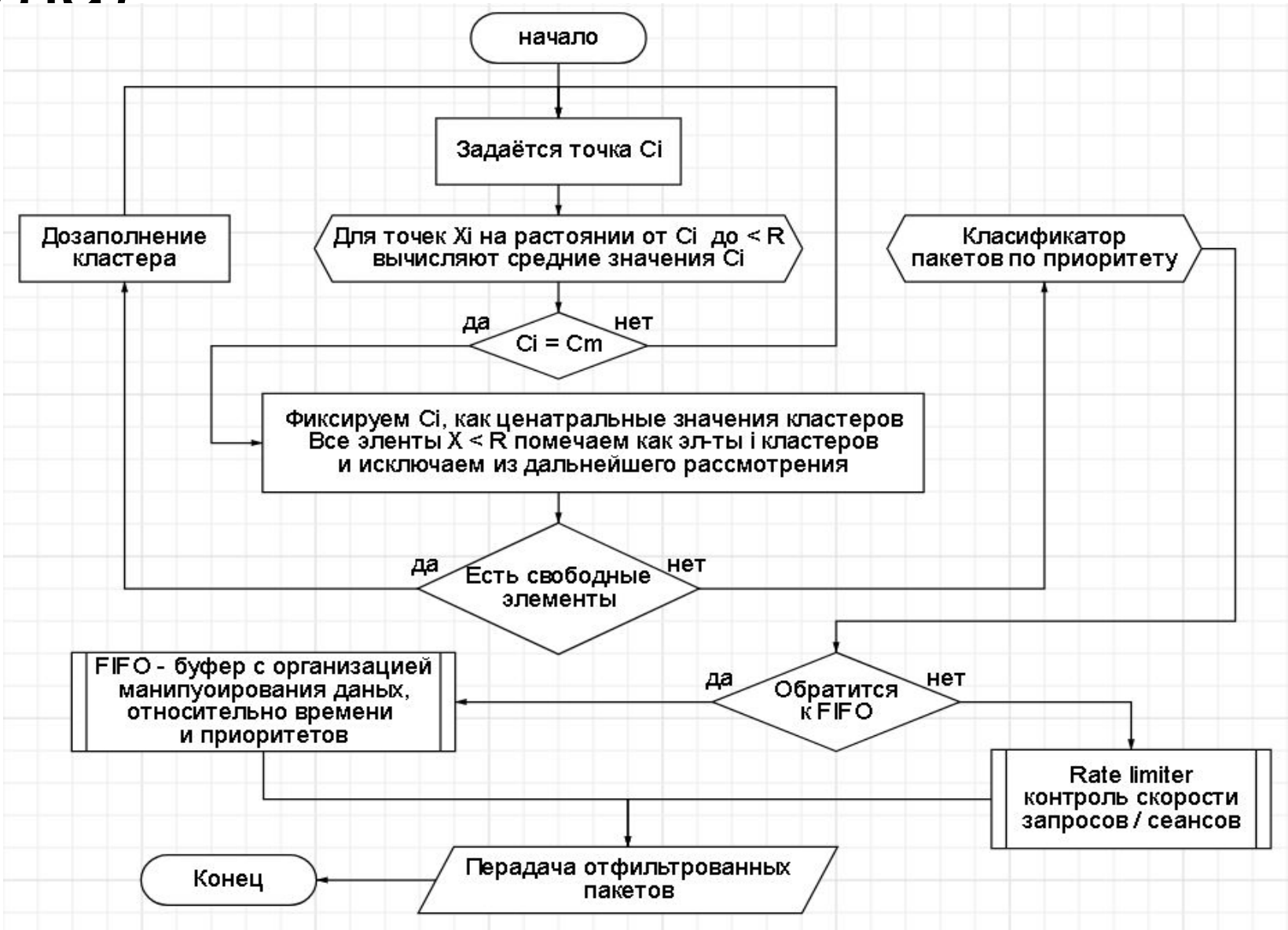
REGNUM — Российские специалисты разрабатывают национальную систему защиты от DDoS-атак, которая должна появится в 2024 году.
Cloudflare — Среди клиентов этого сервиса такие крупные компании, как Nasdaq, DigitalOcean, Cisco.
Akamai — один из лидеров в сфере обеспечения безопасности. По заявлениям руководства, Akamai может справится с атакой в 1,3 терабита в секунду.

Нейтрализация импульсно-волновой DDoS-атаки на линейной скорости

- Метод кластеризации плохо реагирует на удлиненные кластеры.
- Инерция — это не нормализованная метрика: зная, что для такой метрики низкие значения являются лучшими, а ноль — оптимальными. В очень многомерных пространствах, евклидовы расстояния имеют тенденцию становиться раздутыми (это пример так называемого «проклятья размерности»).



Блок-схема алгоритма кластеризации (Ферупа)



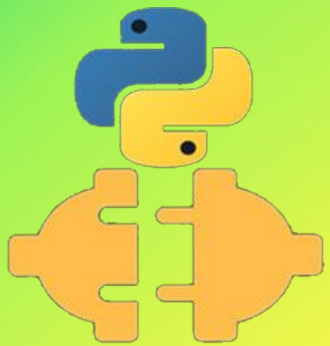
PyCharm 2022.3

Requests

http for humans

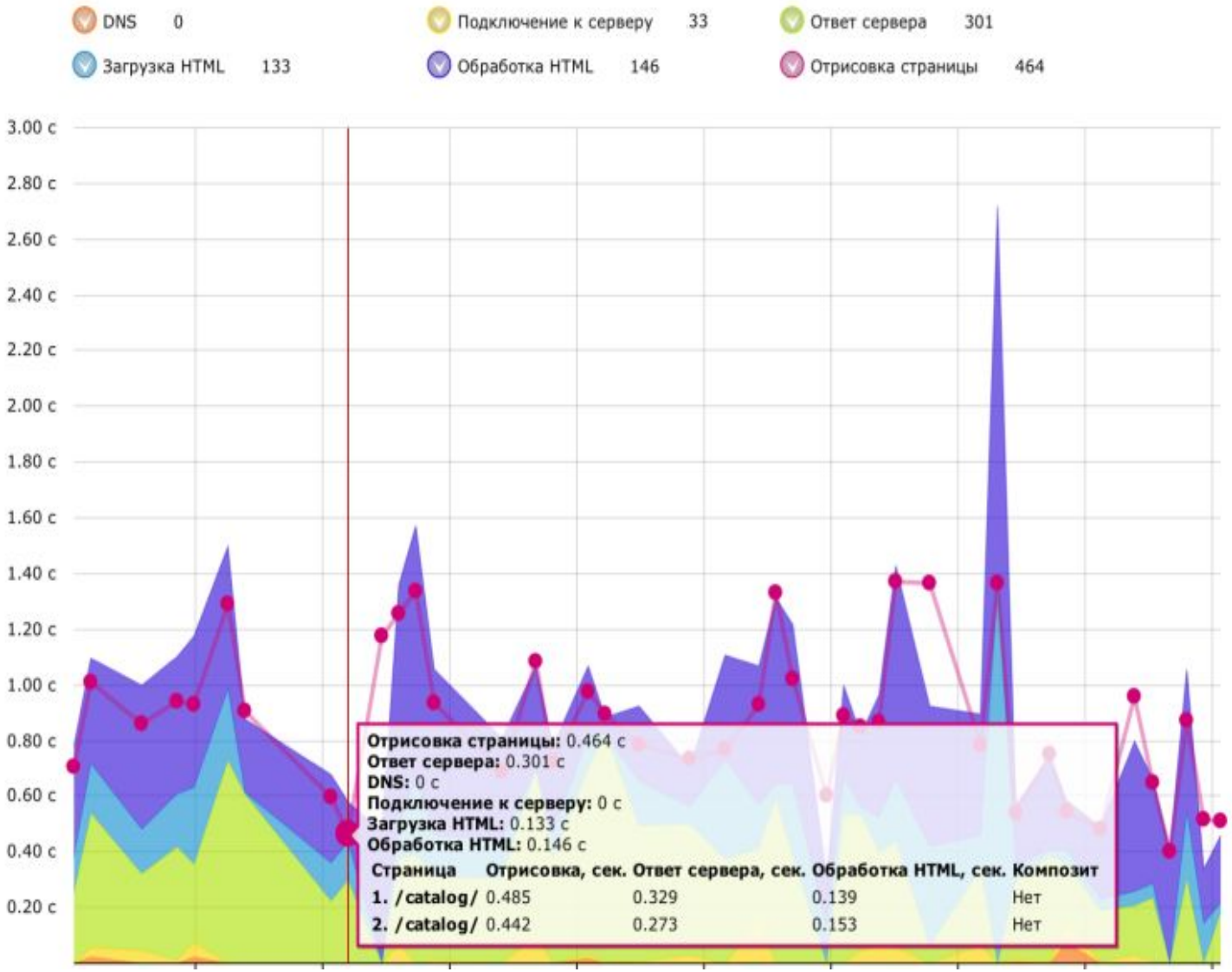
python™

Pandas



PYTHON SOCKET

```
ID кластера:   148 8.2239802120088O4 106.93КБ
ID кластера:   344 7.5833418204847405 436.095КБ
ID кластера:   333 7.4677713517864 98 180.984КБ
ID кластера:   161 7.2915387951064 63 287.952КБ
ID кластера:   380 7.1340753434577 14 329.097КБ
ID кластера:   368 6.855502158454 87 403.096КБ
ID кластера:   152 6.8336202949583 96 403.1КБ
ID кластера:   136 6.819129232495437 510.08КБ
ID кластера:   373 6.8039375853622 74 403.158КБ
ID кластера:   39 6.75743043813825 75 435.889КБ
ID кластера:   382 6.640195163890 02 254.911КБ
ID кластера:   325 6.6254207066133155 361.815КБ
ID кластера:   139 6.593546209798734 328.888КБ
ID кластера:   329 6.507692716385405 370.067КБ
ID кластера:   42 6.495875317563115 328.93КБ
ID кластера:   187 6.1113340113100 09 296.065КБ
ID кластера:   375 6.011005998659481 402.994КБ
ID кластера:   18 5.947889764960214 814.398КБ
ID кластера:   280 5.927041088642917 740.332КБ
ID кластера:   354 5.911223147681239 624.956КБ
ID кластера:   85 5.888051384034708 296.081КБ
ID кластера:   8 5.8808667330374 22 370.117КБ
ID кластера:   96 5.880564610584635 444.115КБ
ID кластера:   19 5.612143236990542 518.603КБ
ID кластера:   390 5.4826149288233 61 403.478КБ
ID кластера:   147 5.3081717278761 43 518.581КБ
ID кластера:   357 5.2600809588652 21 477.453КБ
ID кластера:   250 5.203793662005134 312.726КБ
ID кластера:   310 5.2011491300453745 312.746КБ
ID кластера:   215 5.1916802790393 19 312.48КБ
ID кластера:   21 5.080469519260245 312.849КБ
ID кластера:   388 4.9021639059907 43 279.811КБ
ID кластера:   307 4.893971662725509 279.904КБ
ID кластера:   113 4.8736238516171 58 279.801КБ
ID кластера:   145 4.8599413423518 98 345.608КБ
ID кластера:   186 4.7933520696396 59 255.029КБ
ID кластера:   38 4.776562291696414 345.576КБ
ID кластера:   12 4.745678576901665 345.565КБ
```



Заключение

В дипломной работе были решены следующие задачи:

- проанализированы существующие кибератаки типа DDoS;
- изучены особенности реализации DDoS-атаки импульсно-волнового типа и найден метод их детектирования и частичной нейтрализации;
- реализовано программное средство, по детектированию и противодействию DDoS атак импульсно-волновым методом, для выстраивания механизма обнаружения и защиты.

Проект **Memo4x4** разработка программ
для бизнеса и торговли

ИНН: 616504000525 КПП: 0
Банковские реквизиты:
Юго-Западный банк ПАО "Сбербанк России", г. Ростов-на-Дону
БИК: 046015602 Р/С: 40802810152090000994
К/С: 30101810600000000602 ОГРН: 309616530200056

E-mail: memo4x4@yandex.ru
Сайт: www.memo4x4.ru
Skype: Genricke

АКТ

о внедрении результатов дипломной работы

На тему «Программное средство по обнаружению и противодействию импульсно-волновым DDoS-атакам (pulse wave)»

По направлению 10.05.01 Компьютерная безопасность

По образовательной программе Математические методы защиты информации

Выполненной Ляшенко Кириллом Александровичем

Настоящим актом подтверждается, что в рабочем процессе компании MEMO4X4 используются следующие практические результаты работы Ляшенко Кирилла Александровича:

- разработанный алгоритм кластеризации сетевых пакетов «Ферула», используемый в системе фильтрации трафика на уровне L7 модели OSI;
- разработанное программное средство, которое предназначено для обнаружения и противодействия импульсно-волновым DDoS-атакам (Pulse Wave) на основе разработанного алгоритма кластеризации «Ферула».

Исследовательские результаты разработанного алгоритма и программного средства показали, что данная разработка позволила обеспечить повышение эффективности обнаружения и фильтрации вредоносного трафика, позволяя справляться с импульсно-волновым DDoS-атаками.

Эксплуатация программного средства показала его эффективную и надёжную работоспособность

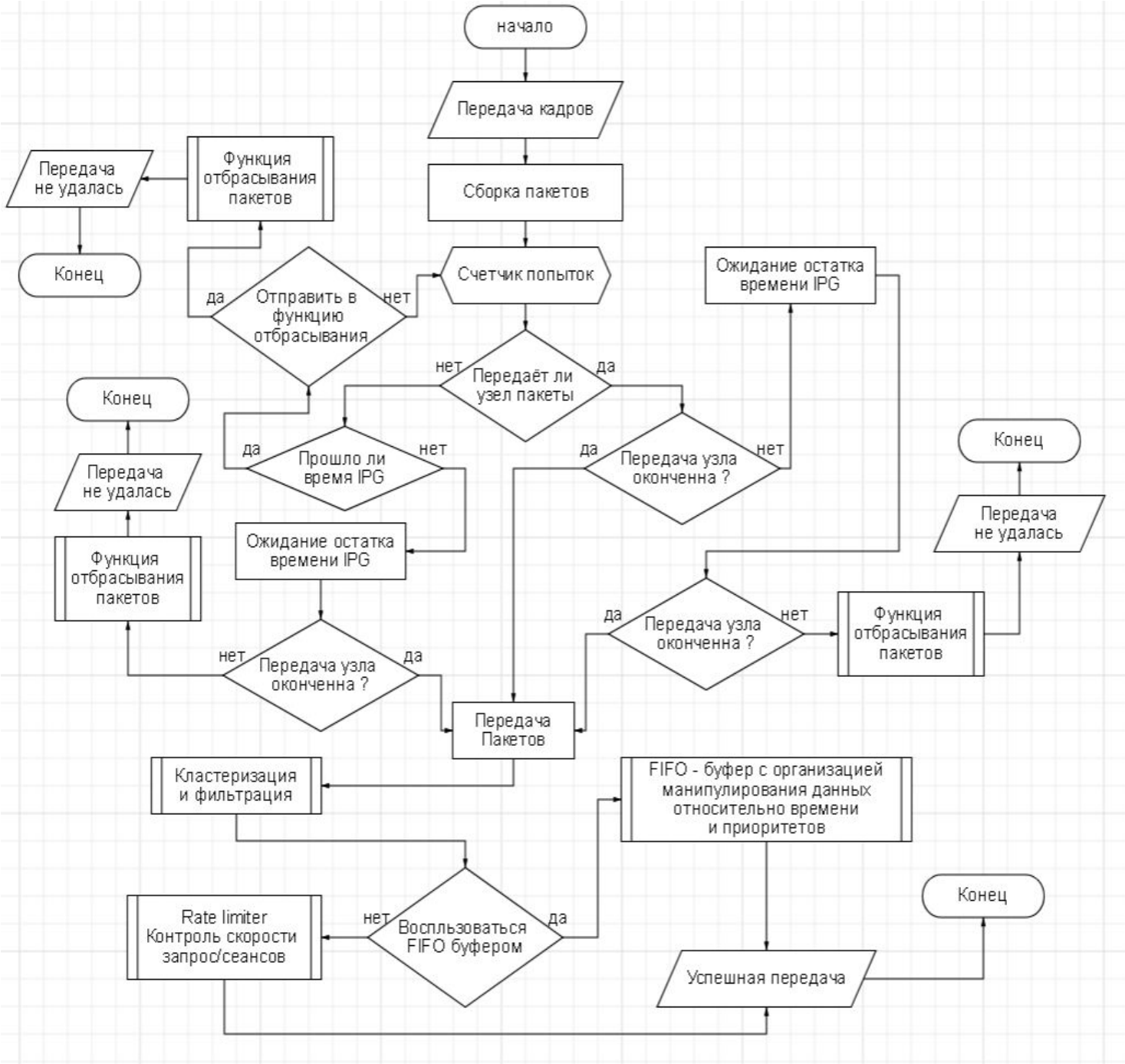
ИП Ляшенко Г.Г. МП

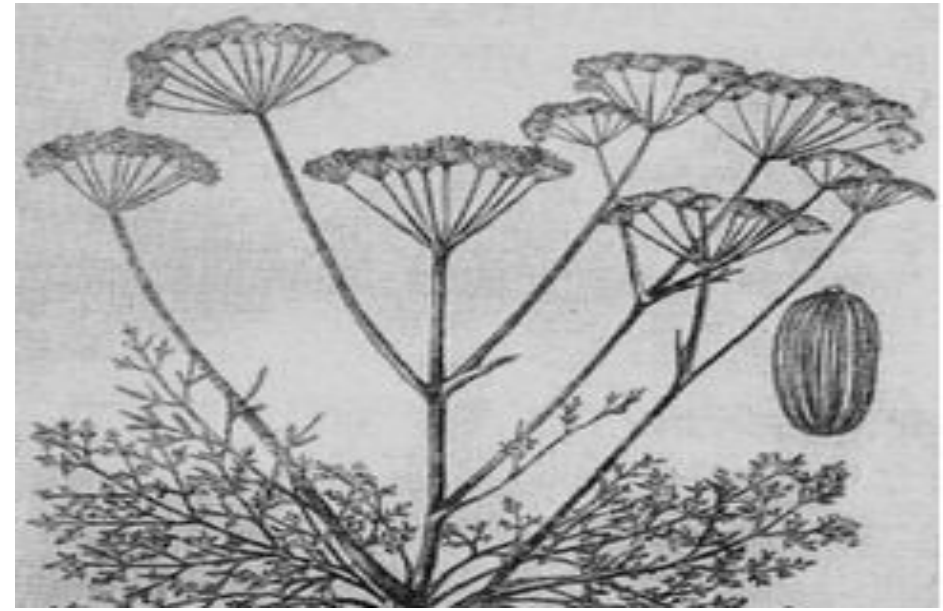
Ляшенко Г.Г.

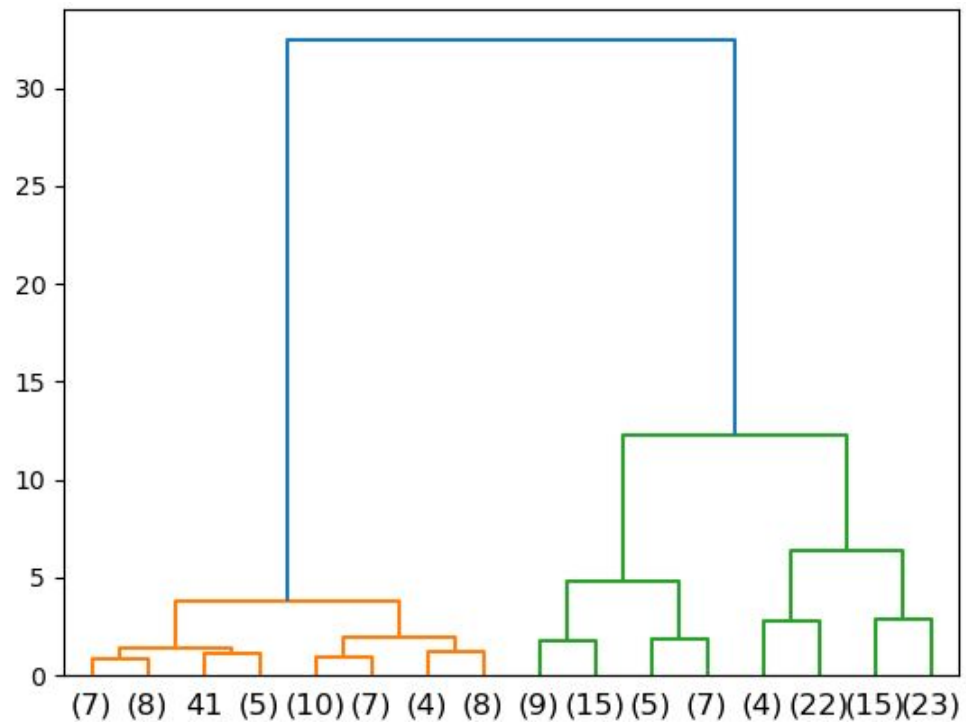
Подпись

Атаки, направленные на переполнение канала (L3)	Атаки, использующие уязвимости стека сетевых протоколов (L4)	Атаки на уровень приложений (L7)
DNS амплификация (DNS Amplification)	ACK / PUSH ACK флуд (ACK & PUSH ACK Flood)	HTTP флуд (HTTP Flood, Excessive VERB)
DNS флуд (DNS Flood)	SYN-ACK флуд (SYN-ACK Flood)	HTTP флуд одиночными запросами (Single Request HTTP Flood, Multiple VERB Single Request)
ICMP флуд (ICMP Flood)	SYN-флуд (SYN Flood)	HTTP флуд одиночными сессиями (Single Session HTTP Flood, Excessive VERB Single Session)
VoIP флуд (VoIP Flood)	Атака поддельными TCP сессиями с несколькими ACK (Multiple ACK Fake Session Attack)	Атака с целью отказа приложения (Faulty Application Attack)
NTP флуд (NTP Flood)	Атака поддельными TCP сессиями с несколькими SYN-ACK (Multiple SYN-ACK Fake Session Attack)	Атака фрагментированными HTTP пакетами (Fragmented HTTP Flood, HTTP Fragmentation)
Ping флуд (Ping Flood)	Атака с помощью перенаправления трафика высоконагруженных сервисов (Misused Application Attack)	Сессионная атака. Атака медленными сессиями (Session Attack, SlowLoris)
UDP флуд (UDP Flood)	Атака поддельными TCP сессиями (Fake Session Attack)	Рекурсивный HTTP GET флуд (Recursive HTTP GET Flood)

Модель					
Уровень (layer)		Тип данных (PDU[15])	Функции	Примеры	Оборудование
Host layers	7. Прикладной (application)	Данные	Доступ к сетевым службам	HTTP, FTP, POP3, WebSocket	Хосты (клиенты сети), Межсетевой экран
	6. Представления (presentation)		Представление и шифрование данных	ASCII, EBCDIC, JPEG, MIDI	
	5. Сеансовый (session)		Управление сеансом связи	RPC, PAP, L2TP, gRPC	
	4. Транспортный (transport)	Сегменты (segment) / Датаграммы (datagram)	Прямая связь между конечными пунктами и надёжность	TCP, UDP, SCTP, Порты	
Media[16] layers	3. Сетевой (network)	Пакеты (packet)	Определение маршрута и логическая адресация	IPv4, IPv6, IPsec, AppleTalk, ICMP	Маршрутизатор, Сетевой шлюз, Межсетевой экран
	2. Канальный (data link)	Биты (bit)/ Кадры (frame)	Физическая адресация	PPP, IEEE 802.22, Ethernet, DSL, ARP, сетевая карта.	Сетевой мост, Коммутатор, точка доступа
	1. Физический (physical)	Биты (bit)	Работа со средой передачи, сигналами и двоичными данными	USB, RJ («витая пара», коаксиальный, оптоволоконный), радиоканал	Концентратор, Повторитель (сетевое оборудование)


начало
Передача кадров
Сборка пакетов
Счетчик попыток
Отправить в функцию отбрасывания
да
нет
Функция отбрасывания пакетов
Передача не удалась
Конец
Передаёт ли узел пакеты
нет
да
Прошло ли время IPG
да
нет
Ожидание остатка времени IPG
Передача узла окончена ?
да
нет
Ожидание остатка времени IPG
Конец
Передача не удалась
Функция отбрасывания пакетов
Передача узла окончена ?
нет
да
Передача узла окончена ?
да
нет
Функция отбрасывания пакетов
Конец
Передача не удалась
Передача Пакетов
Кластеризация и фильтрация
FIFO - буфер с организацией манипулирования данных относительно времени и приоритетов
Rate limiter Контроль скорости запрос/сеансов
нет
Воспользоваться FIFO буфером
да
Конец
Успешная передача




30
25
20
15
10
5
0
(7) (8) 41 (5) (10) (7) (4) (8) (9) (15) (5) (7) (4) (22) (15) (23)

```
PS H:\Diplom\app> python app.py
Допуск достигнут на шаге 2

Завершено итераций: 2
Окончательная перекрестная проверка: 31.631899
k-среднии, 0 , 1 , 31.63189892803241  минимальная ошибка
key-кластер: 1 итераций: 0
Допуск достигнут на шаге 2

Завершено итераций: 2
Окончательная перекрестная проверка: 31.631899
k-среднии, 1 , 1 , 31.63189892803241  минимальная ошибка
key-кластер: 1 итераций: 1
Допуск достигнут на шаге 2

Завершено итераций: 11
Окончательная перекрестная проверка: 2.590740
Ferula, 18 , 3.283351195112404 , 2.4834738410136556 ,Итерац
Ferula_method итерация: 18
Допуск достигнут на шаге 15

Завершено итераций: 15
Окончательная перекрестная проверка: 2.583735
Ferula, 19 , 3.283351195112404 , 2.4834738410136556 ,Итерац
Ferula_method итерация: 19 10.00000
Ferula, 3.283351195112404 , 2.4834738410136556 ,
4733.092500000005
Допуск достигнут на шаге 14

Завершено итераций: 14
Окончательная перекрестная проверка: 3.903586
Ferula, 0 , 4.53770277460442 , 3.9035857731919963 ,Итерация
Ferula_method итерация: 0
Допуск достигнут на шаге 14
```