УДК 004

В. В. Храмов[1] *

Модуль для анализа и выявления аномального трафика для противодействия распределенным атакам типа «отказ в обслуживании»

[1] Национальный исследовательский ядерный университет «МИФИ», г. Москва, Российская Федерация
* e-mail: xramow.vova2015@yandex.ru

Аннотация. В статье представлена методика реализации модуля для анализа и выявления аномального трафика для противодействия распределенным атакам типа «отказ в обслуживании». Объектом исследования является средства анализа и выявления вредоносного трафика. Целью работы является обеспечение доступности сервера путем блокировки аномального трафика в период атаки. В ходе работы были классифицированы атаки типа «отказ в обслуживании». Для каждого класса были выделены отдельные методы противодействия. Каждая компонента модуля является изолированной при помощи Docker в связке с балансировщиком нагрузки на Nginx. Эффективность управления данным модулем достигается за счет автоматизированного развертывания всех компонентов при помощи системы управления конфигурациями Ansible. В результате работы были построены BPMN-диаграммы предметной области. В ходе проектирования и программной реализации модуля были построены UML-диаграммы деятельности и блок-схемы алгоритмов для каждого компонента модуля. Результаты тестирования были оформлены в виде диаграмм и таблиц. Предлагаемый модуль предоставляет возможность анализа и выявления аномального трафика на каждом этапе работы модуля.

Ключевые слова: отказ в обслуживании, iptables, балансировка нагрузки, фильтрация трафика

V. V. Khramov[1] *

Module for analyzing and detecting anomalous traffic to counter distributed denial-of-service attacks

[1] National research nuclear university “MEPhI”, Moscow, Russian Federation
* e-mail: xramow.vova2015@yandex.ru

Abstract. The article presents a methodology for implementing a module for analyzing and detecting anomalous traffic to counter distributed denial-of-service attacks. The object of the study is the means of analyzing and detecting malicious traffic. The aim of the work is to ensure server availability by blocking anomalous traffic during the attack period. In the course of the work, denial of service attacks have been categorized. Separate countermeasure methods were identified for each class. Each component of the module is isolated using Docker in conjunction with a load balancer on Nginx. The efficiency of managing this module is achieved by automated deployment of all components using Ansible configuration management system. As a result of the work BPMN diagrams of the subject area were built. During the design and program implementation of the module UML activity diagrams and algorithm flowcharts for each component of the module were built. The results of testing were formalized in the form of diagrams and tables. The proposed module provides the ability to analyze and detect anomalous traffic at each stage of the module operation.

Keywords: denial of Service, iptables, load balancing, traffic filtering

Введение

Информационные технологии являются неотъемлемой частью современного мира. Они присутствуют практически в каждом аспекте человеческой жизни. Их развитие также не стоит на месте и становится более прогрессивным. Однако вместе с этими возможностями возникают и новые задачи, такие как обеспечение конфиденциальности, целостности и доступности информации [1, 2, 3]. Данная тенденция обусловлена ростом киберпреступности и необходимостью защиты данных. К примеру, только за последние 3 года количество атак типа «отказ в обслуживании» возросло в 4 раза [4] и за последний квартал 2023 года составило 331 тыс. В связи с этим растет важность разработки систем противодействия таким типам атак.

Научное сообщество также занимается вопросом изучения различных методов противодействия атакам типа «отказ в обслуживании». Исследованием флудовых атак занимаются Taghavi Zargar, James Joshi, David Tipper [5]. Рассматриваемые подходы эффективно работают для защиты от ddos-атак типа флуд, однако это лишь одна из разновидностей атак на отказ в обслуживании. Также существуют более комплексные подходы к изучению этого вопроса [6, 7]. Данный механизм основан на анализе аномалий в трафике, что позволит противодействовать флудовым атакам, атакам на заполнение буфера и пропускного канала. Однако данный механизм не предполагает автоматическое развертывание системы и управление ею, что затруднит процессы рефакторинга и масштабирования.

Федеральная служба по техническому и экспортному контролю разработала приказ от 25 декабря 2017 г. N 239 об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации [8]. Требования, устанавливаемые приказом, обязуют обеспечить безопасность значимых объектов критической информационной инфраструктуры Российской Федерации, в том числе и от атак типа «отказ в обслуживании».

Исходя из рассмотрения актуальности вопроса защиты от ddos-атак с различных сторон, можно сделать вывод о том, что актуальность данной проблемы стремительно растет.

Целью настоящей работы является реализация автоматизированного модуля противодействия распределенным атакам типа «отказ в обслуживании», обеспечивающего доступность веб-сервисов.

Разработанный модуль позволит обеспечить защиту от основных видов атак типа «отказ в обслуживании», а также предоставит возможность эффективного управления конфигурациями его составных компонентов и автоматизированной развертки.

Методы и материалы

В этом разделе будет проведен сравнительный анализ серверов и пакетных фильтров, а также проектирование и программная реализация автоматизирован-

ного модуля для противодействия распределенным атакам типа «отказ в обслуживании».

Основными компонентами модуля являются серверы, сетевые пакетные фильтры и скрипт для поиска аномалий в трафике. Для исследования и сравнения существующих решений был развернут виртуальный тестовый стенд на базе kali-linux 2024. Основными критериями для сравнения серверов являются скоростные характеристики, а также вариативность методов балансировки нагрузки. Результаты сравнения серверов представлены в табл. 1.

Таблица 1

Сравнительный анализ веб-серверов

Веб-сервер	Скорость обработки, пакетов в секунду	Скорость передачи данных (Кбайт/с)	Количество методов балансировки нагрузки
Nginx	19318	205936	7
Apache	7479	79949	3
LiteSpeed	11744	160275	3
Caddy	6395	72759	4

В качестве основных критериев оценки пакетных фильтров были также выбраны скоростные характеристики, возможность противодействия ddos и взаимодействие с веб-серверами. Результаты тестирования представлены в табл. 2.

Таблица 2

Сравнительный анализ пакетных фильтров

Пакетные фильтры	Скорость обработки, пакетов в секунду	Классовая оценка противодействия ddos (1-5 классов)
iptables	12478	3
Firewalld	11899	1
Fail2Ban	13284	1
Modsecurity (apache module)	5027	3

В ходе моделирования предметной области была построена BPMN-диаграмма взаимодействия администратора с модулем (рис. 1). Основными этапами данной диаграммы являются процессы настройки и конфигурирования необходимых компонентов модуля.

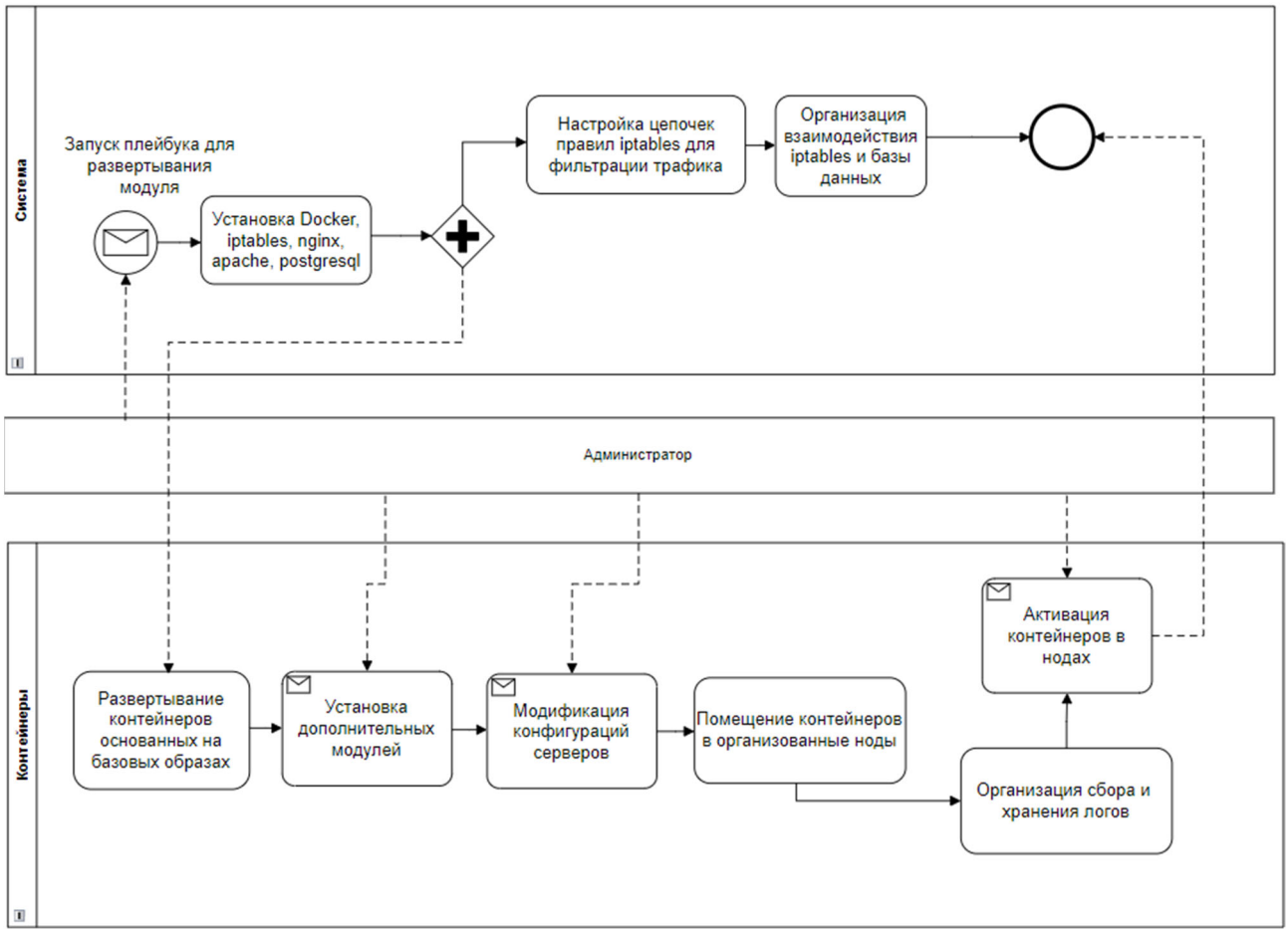

Рис. 1. BPMN-диаграмма взаимодействия администратора с модулем.

Для реализации проектирования модуля защиты был выбран следующий стек технологий:

– Apache2 – обработка динамических данных, противодействие атакам на прикладном уровне;

– Nginx – балансировка нагрузки, обработка статических данных и противодействие медленным атакам;

– Postgresql – хранение потенциально опасных ip-адресов;

– Iptables – конфигурирование цепей правил защиты от ddos-атак на сетевом уровне [9, 10];

– Ansible и Vagrant – автоматизация конфигурирования и настройки правил;

– Docker – изоляция каждого компонента модуля;

– Python – детектирование и обработка аномального трафика [11, 12, 13, 14].

На UML-диаграмме деятельности (рис. 2) визуализирован процесс конфигурирования и запуска модуля.

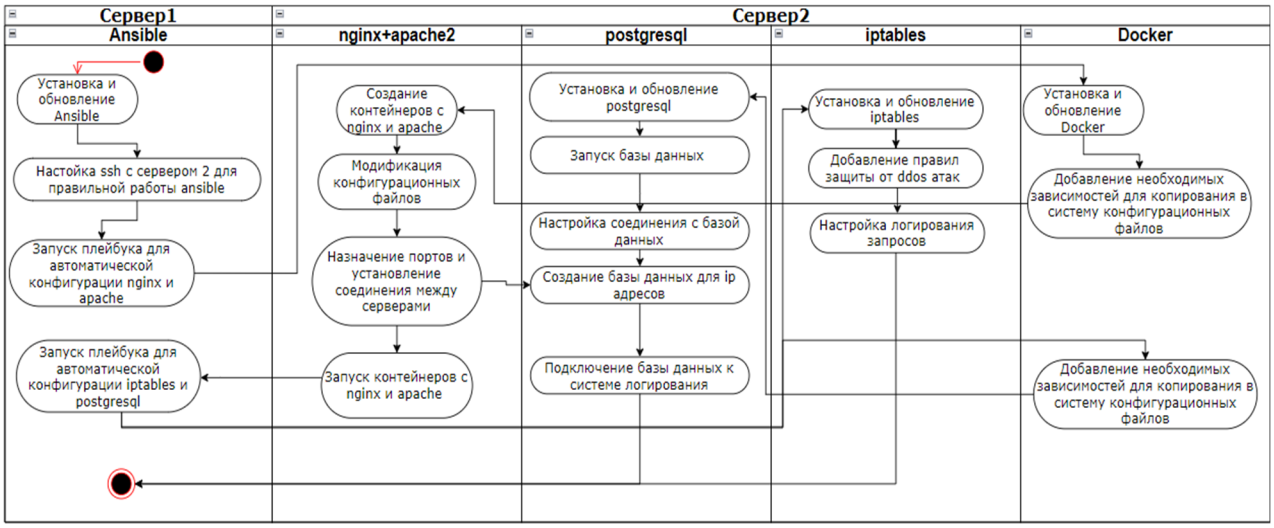

Рис. 2. UML-диаграмма деятельности конфигурирования

Процесс развертывания модуля можно разделить на основные этапы:

Сервер 1

– установка и настройка ansible для управляющей машины, а также соединения с защищаемой машиной [15];

– ansible-playbook для создания цепочки нодов;

– ansible-playbook для конфигурирования компонентов модуля;

Сервер 2

– установка и запуск Docker;

– импорт необходимых конфигураций;

– создание образов контейнеров, адаптированных под каждый компонент модуля;

– создание контейнеров с заданными конфигурациями;

– загрузка и запуск контейнеров в подходящих нодах;

– импорт и запись правил iptables.

В ходе программной реализации модуля была построена блок-схема алгоритма (рис. 3). Данная блок-схема представляет собой процесс обработки запросов.

При попадании пакета в систему он проходит проверку по правилам iptables. В случае успешного прохождения всех цепей правил пакет допущен к дальнейшей обработке. Иначе пакет отбрасывается и логируется.

На сервере nginx пакет проверяется на медленные атаки, а также на атаки на заполнение буфера. Далее осуществляется проверка расширения файла запроса, исходя из которой сервер понимает, динамический или статический трафик нужно передать. В случае динамического трафика запрос балансируется на сервера apache, иначе обрабатывается самим nginx.

На сервере apache пакет проходит проверку модулями mod_security и mod_evasive. В случае успешной проверки запрос логируется и обрабатывается. Иначе пакет отбрасывается.

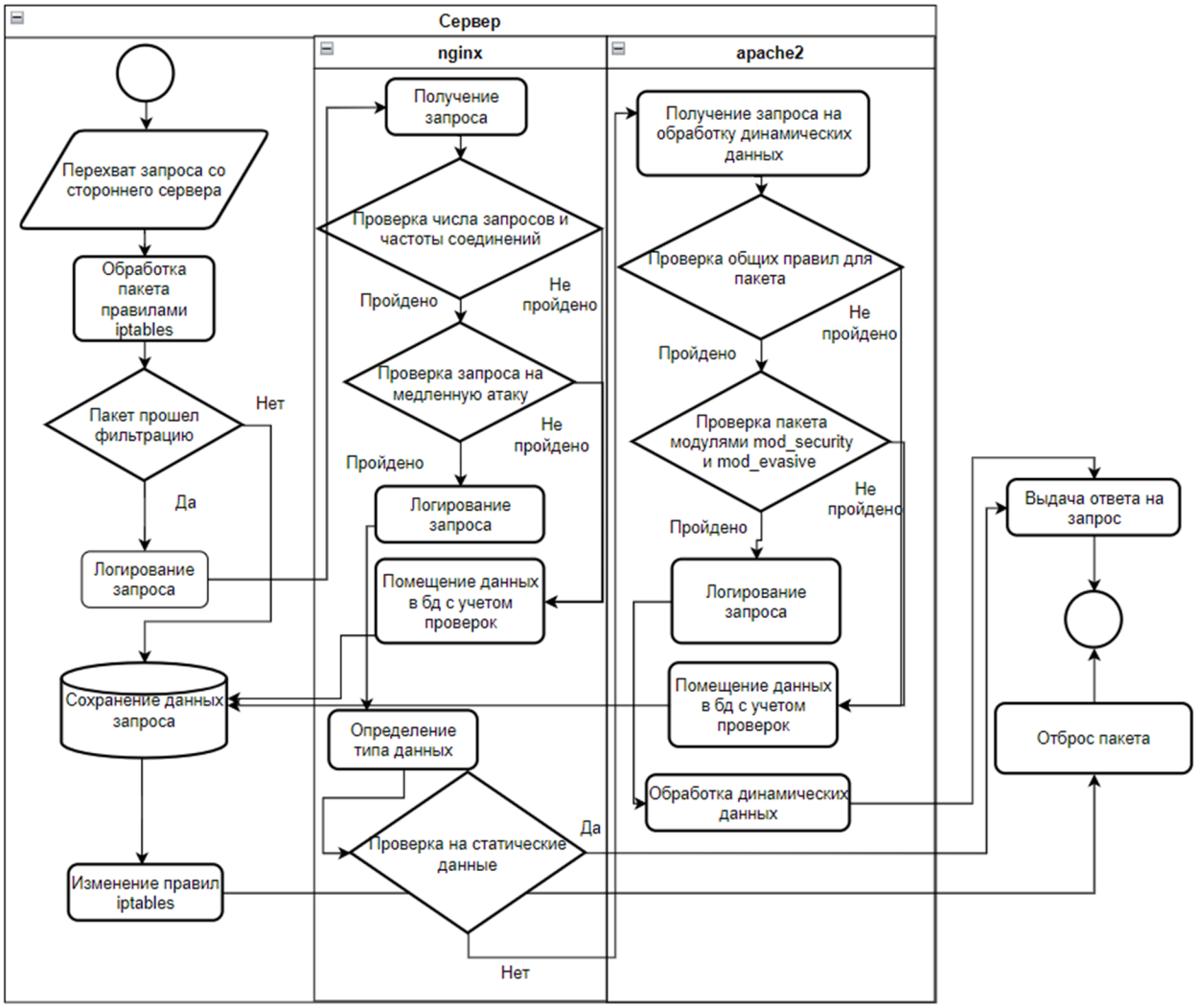

Рис. 3. Блок-схема работы модуля

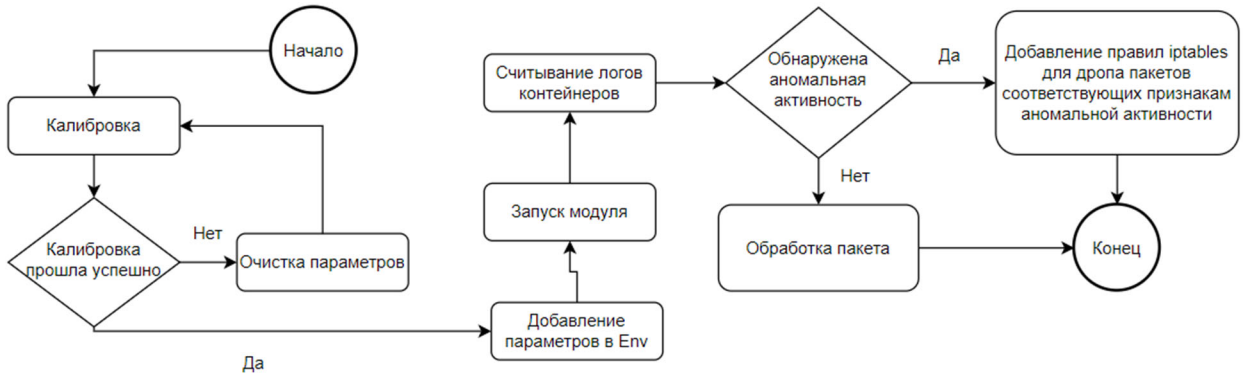

Рис. 4. Блок-схема алгоритма анализа трафика

Следующим компонентом модуля является python-скрипт, анализирующий трафик, который прошел все вышеуказанные проверки. Основой данного алгоритма является статистические данные, полученные в ходе нормальной работы

серверов. В случае атаки эти показатели нарушаются, что незамедлительно вызывает блокировку пакетов, нарушающих нормальные показатели. Данный алгоритм визуализирован и представлен на рис. 4.

Такой алгоритм анализа трафика позволит комплексно выявлять ddos-атаки, а также за счет калибровки адаптироваться под любую систему.

Тестирование

В ходе тестирования модуля на виртуальном стенде были апробированы базовые классы атак типа «отказ в обслуживании». Также полученные результаты были проанализированы и оформлены в виде графика (рис. 5).

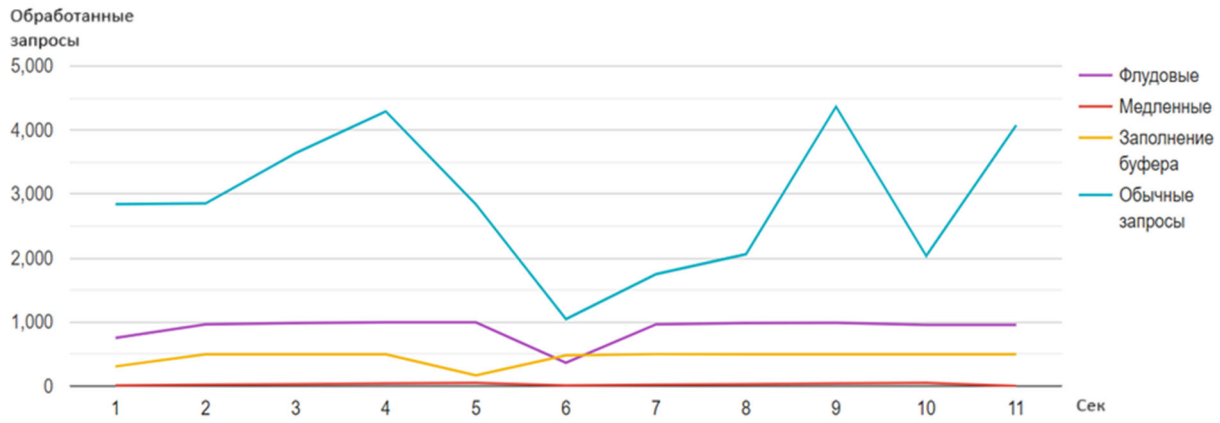

Рис. 5. График влияния атак на систему

По итогам анализа, можно отметить, что все проводимые атаки были успешно предотвращены без влияния на нормальное функционирование системы.

Заключение

В работе был представлен многокомпонентный автоматизированный модуль анализа и выявления аномального трафика для противодействия распределенным атакам типа «отказ в обслуживании». Особенностью данного модуля является полная автоматизация его конфигурирования, а также способность противодействовать базовым классам ddos-атак. Эти преимущества позволяют эффективно и быстро изменять конфигурацию модуля, а также масштабировать его.

В ходе работы было проведено исследование предметной области, анализ и сравнение существующих решений. Были получены экспериментальные данные и представлены в виде таблиц. В результате моделирования была построена BPMN-диаграмма, отражающая этапы взаимодействия администратора с модулем. При проектировании предметной области были построены UML-диаграммы автоматизированного конфигурирования, представляющие настройку основных компонентов модуля. В ходе программной реализации были построены блок-

схемы алгоритмов, отражающие процесс взаимодействия систем, а также процесс предотвращения атак типа «отказ в обслуживании». Было проведено тестирование модуля на виртуальном стенде, по результатам которого все проводимые атаки успешно отражены.

Таким образом, автоматизированный модуль для анализа и выявления аномального трафика является важным дополнением в системах безопасности сети.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Басыня Е. А. Метод управления трафиком на межсетевых узлах локальных вычислительных сетей // Известия Самарского научного центра Российской академии наук. – 2014. – Т. 16. – №. 4-3. – С. 507-511.

2. Белышева Ю. И. Исследование типов ddos атак // Сборник статей LXIII Международной научно-практической конференции “World science: problems and innovations”. Ответственный редактор. – 2022. – С. 54.

3. Камышев С. В., Карманов И. Н. Проблемы DDoS-атак в современной IT-индустрии и методы защиты от них // Интерэкспо Гео-Сибирь. – 2018. – №. 9. – С. 121-125.

4. Тенденции DDoS-атак в 2023 году. – URL: https://ddos-guard.net/ru/blog/tendentsii-ddos-atak-2023

5. Zargar S. T., Joshi J., Tipper D. A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks // IEEE communications surveys & tutorials. – 2013. – Т. 15. – №. 4. – С. 2046-2069.

6. Басыня Е. А. Сетевая информационная безопасность и анонимизация. – Litres, – 2022. – С. 75.

7. Зирнис Л. С., Новикова Т. П. Методика борьбы с ddos-атаками // Новые аспекты моделирования систем и процессов. – 2023. – С. 330.

8. Приказ ФСТЭК России от 25 декабря 2017 г. N 239 [Электронный ресурс] – Доступ к ресурсу URL: https://fstec.ru/dokumenty/vse-dokumenty/prikazy/prikaz-fstek-rossii-ot-25-dekabrya-2017-g-n-239

9. Руководство по Iptables 1.1.19. – URL: https://www.opennet.ru/docs/RUS/iptables.

10. Пальчевский Е. В., Халиков А. Р. Разработка системы блокировки трафика посредством фильтра IPTABLES // Составители: Научно-издательский центр «Мир науки». – 2017.

11. Краснов А. Е. и др. Детектирование DDoS атак на основе анализа динамики и взаимосвязи характеристик сетевого трафика // Вестник Удмуртского университета. Математика. Механика. Компьютерные науки. – 2018. – Т. 28. – №. 3. – С. 407-418.

12. Бачманов Д. А. и др. Сравнение подходов к идентификации процесса реализации распределенной атаки типа «Отказ в обслуживании» // Цифровые технологии и защита информации в современном обществе. – 2021. – С. 56-60.

13. Корякова В. А. Определение распределенных атак типа «Отказ в обслуживании» на основе анализа параметров сетевых пакетов // Цифровые технологии и защита информации в современном обществе. – 2021. – С. 40-45.

14. Rohit M. H., Fahim S. M., Khan A. H. A. Mitigating and detecting ddos attack on iot environment // 2019 IEEE International Conference on Robotics, Automation, Artificial-intelligence and Internet-of-Things (RAAICON). – IEEE, 2019. – С. 5-8.

15. Басыня Е. А., Лукина М. С. Автоматизированная установка и конфигурирование серверных решений // Современные материалы, техника и технологии. – 2016. – №. 2 (5). – С. 21-26.