МЕТОД ИДЕНТИФИКАЦИИ СЕТЕВЫХ АТАК С ИСПОЛЬЗОВАНИЕМ ЭФФЕКТИВНЫХ ХАРАКТЕРИСТИК СТАТИСТИЧЕСКИХ МЕТОДОВ

З.Н. Пенчев, А.В. Мансуров
Алтайский государственный университет, г. Барнаул

Атаки отказа в обслуживании (DoS) и атаки распределенного отказа в обслуживании (DDoS) стали большой проблемой для пользователей компьютерных систем, подключенных к сети Интернет. Таким образом, защита компьютерных систем от подобного вида атак является приоритетной задачей.

На данный момент существует три решения против DoS/DDoS-атак: предотвращение, обнаружение и реакция. Обнаружение является одним из важных шагов в защите от DoS/DDoS-атак.

Существует несколько основных подходов к определению DoS-атак:

1. Методы машинного обучения [1-2,8];
2. Методы мультифрактального анализа [3-5,9];
3. Статистические методы [6-7,11-12].

Подход с использованием машинного обучения автоматически обнаруживает DoS трафик с помощью обученных моделей. Методы нахождения аномальной активности, основанные на модели «нормального» трафика, обнаруживают атаки как значительное отклонение от модели. Если выявлена аномалия, то трафик исследуется дальше. Если какая-то из характеристик превышает «нормальное» значение, полученное во время обучения, то этот поток будет изолирован.

Машинное обучение похоже на статистический метод, но, в данном случае, трафик обрабатывает нейронная сеть, которую надо обучить. В частности, метод [8] использует большое количество преобразований трафика в вид, удобный для нейронной сети. Примерный алгоритм работы выглядит следующим образом:

1. Преобразовать многомерные данные трафика TCP/IP в виде изображения;
2. Классифицировать изображение;
3. Обучить модель;
4. Спрогнозировать модель;
5. Найти эффективные характеристики;
6. Оценить эффективность.

Методы мультифрактального анализа, представленные в публикации [9], оперируют самоподобием сетевого трафика. Для более точной оценки коэффициента самоподобия используется понятие коэффициент Херста. Если коэффициент Херста $H = 0.5$ – полностью случайный процесс без выраженной тенденции. Если коэффициент Херста находится в пределах от $0 < H < 0.5$, то процесс является переменным. Если $H > 0.5$ – трендоустойчивый процесс, который обладает длительной памятью и является самоподобным.

В работе [10] автор предлагает свой метод исследования трафика. Анализируя представленный метод можно сказать, что метод перегружен математическими расчётами. При этом, нужно достаточно больше место, для хранения трафика. Примерный план работы алгоритма:

1. Захват сетевого трафика;
2. Обновление трафика в сети;
3. Обновление вейвлет-коэффициентов;
4. Обновление информационного критерия Шварца;
5. Обнаружение граничной точки в каждом масштабе;
6. Оценка показателя Херста и скорости его изменения;
7. Нечеткие адаптивные решающие правила;
8. Определение интенсивности атаки;
9. Оценка безопасности.

На деле такой метод требует больших вычислительных мощностей и огромного количество памяти, для хранения трафика.

Статистический метод анализа трафика состоит в том, что сопоставляется текущее состояние сети с некими определенными заранее признаками, которые соответствуют штатной работе информационной системы [11, 12]. Данные признаки формируются в некий профиль. После этого, весь входящий трафик разбивается на окна разной длины и сверяется с профилем. Если находятся какие-то отклонения признаков в профиле, то данный трафик отбрасывается. Для этого нам даже не нужны знания о видах атак, так как можно определять даже впервые реализуемые методы вредоносного воздействия.

Данный метод не требует больших вычислительных мощностей, так как сравниваются лишь определенные поля. Нет необходимости в большом количестве математических вычислений, которые применяются в других методах анализа трафика. Ещё одна положительная сторона методики – нужен всего лишь один эталонный образец трафика. Имея эталонный трафик не надо обучать метод на образцах DoS-трафика. Если в сети будет присутствовать аномалия, то метод сможет её распознать.

Огромным преимуществом данного метода является гибкость настраиваемых параметров и временных окон. Каждая атака имеет свой уникальный паттерн – совокупность срабатываемых аномальных признаков. Если срабатывают определенные признаки, то можно даже классифицировать атаку, для более успешной защиты от неё. Также можно настраивать и временные окна сканирования трафика. Если нужно сканировать большое количество трафика, то выбирается одно временное окно, а если количество трафика не имеет значение, то можно взять маленькое временное окно.

Недостатком метода является небольшая задержка, которая присутствует при передаче трафика с коммутатора на устройство, которое будет исследовать трафик.

Предлагается следующий метод определения DoS/DdoS атак, схема которого представлена на рисунке 1.

Ход работы алгоритма:

1. Захват сетевого трафика окнами по 3 секунды;
2. Сохранение трафика в формате CSV;
3. Вычисление среднего времени сессии, энтропии длительности сессии, энтропии уникальных IP-адресов источника, энтропии соединений с сервером.
4. Сравнение вычисленных характеристик захваченного трафика, с характеристиками эталона и выдача ответа о присутствии или отсутствии атаки.

Метод работает следующим образом: трафик, поступающий с маршрутизатора, захватывается окнами по 3 секунды. После этого он конвертируется в формат CSV. Данный файл отправляется на анализ в алгоритм, который высчитывает следующие характеристики: среднее время сессии; энтропия длительности сессии, энтропия уникальных IP-адресов источника, энтропия соединений с сервером. После этого просчитанные характеристики попадают на блок сравнения, где они сравниваются с эталонными значениями легитимного трафика. В конце сравнения выдается заключение о типе трафика.

Предлагаемый метод апробирован на 13 наборах реального и модельного трафика. Этот этап позволил установить минимальный размер рабочего «окна» для метода и выявить основные чувствительные к характеру сетевого трафика в выбранном окне характеристики.

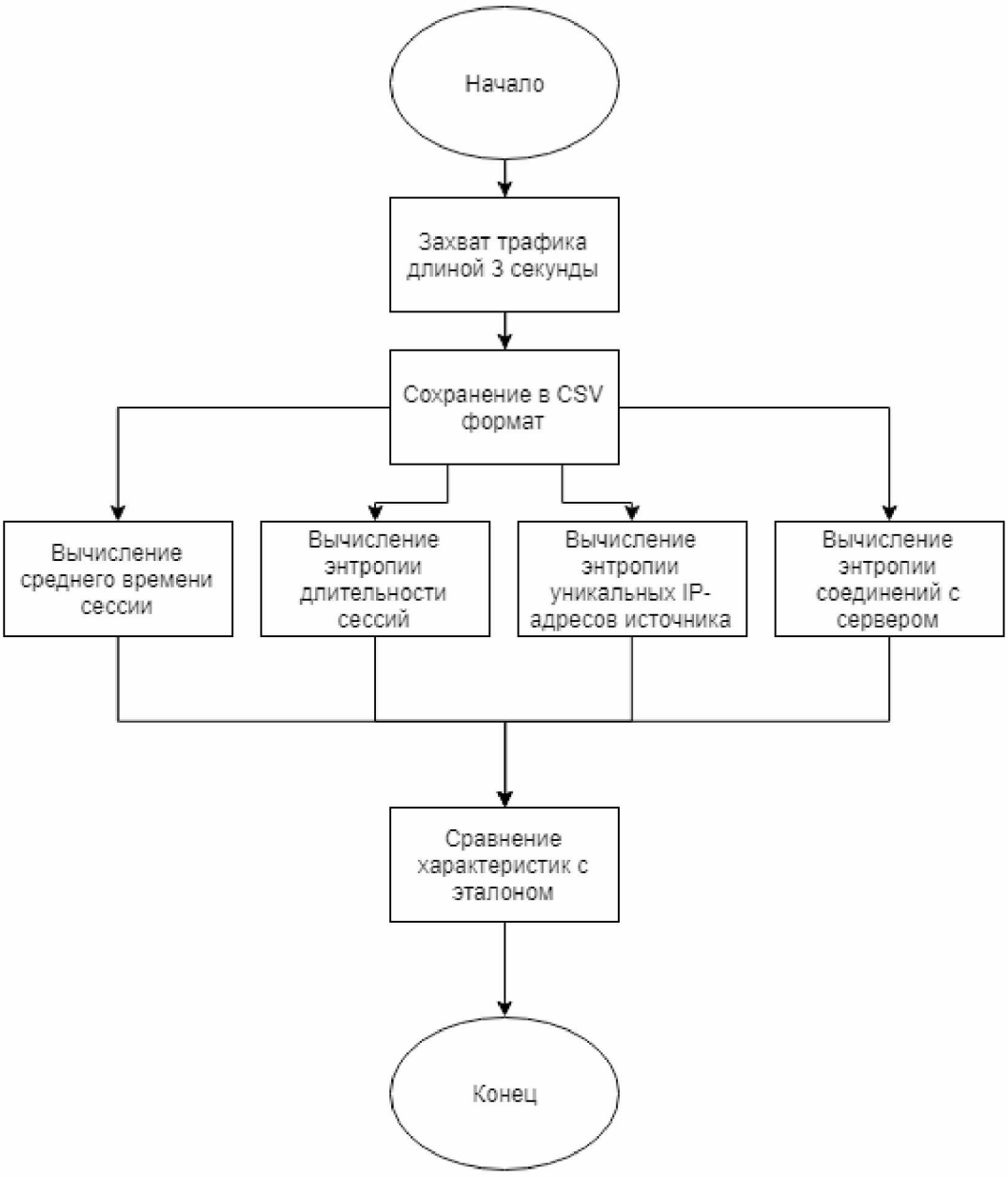

Рисунок 1 – Блок схема предлагаемого метода

Реальный трафик захватывается одним большим файлом, длительностью в 10 минут. После этого преобразуется в CSV формат и делится на временные окна. Образцы захваченного трафика:

- Трафик работы небольшой локальной сети (6 машин);
- Трафик работы сервера игры «Minecraft»;
- BitTorrent трафик;
- DoS-трафик;
- SYN-flood трафик.
- Сгенерировано 4 образца модельного трафика:
- Модельный трафик подключения к серверу с местных IP-адресов;
- Модельный трафик подключения к серверу с российских IP-адресов;
- Модель DoS-атаки;
- Модель SYN-flood.

Для имитации работы реальной сети были скомбинированы следующие наборы трафика:

- Локальная сеть + сервер;
- Локальная сеть + BitTorrent;

- Локальная сеть + DoS-атака;
- Локальная сеть + SYN-flood.

В начале рассматриваются характеристики модельного трафика. Для исследования трафика используются «окна» с различным интервалом (от 10 минут до 3 секунд). Длительность окна подбирается в ходе исследования автоматически, путем кратного уменьшения времени окна. Вычисляются показатели среднего времени сессии и энтропийные показатели.

Анализируя все временные «окна» для модельного трафика, можно сделать вывод, что лучшим «окном», для определения атак, является окно в 3 секунды. На рисунке 2 показано, что, начиная с третьей секунды захвата, некоторые виды трафика можно отличать друг от друга. Рисунок 3 демонстрирует, что с помощью энтропии уникальных IP-адресов источника, можно точно определять виды трафика, также с 3 секунд. Рисунок 4 подтверждает возможность определения 2 других видов трафика, начиная с трех секунд.

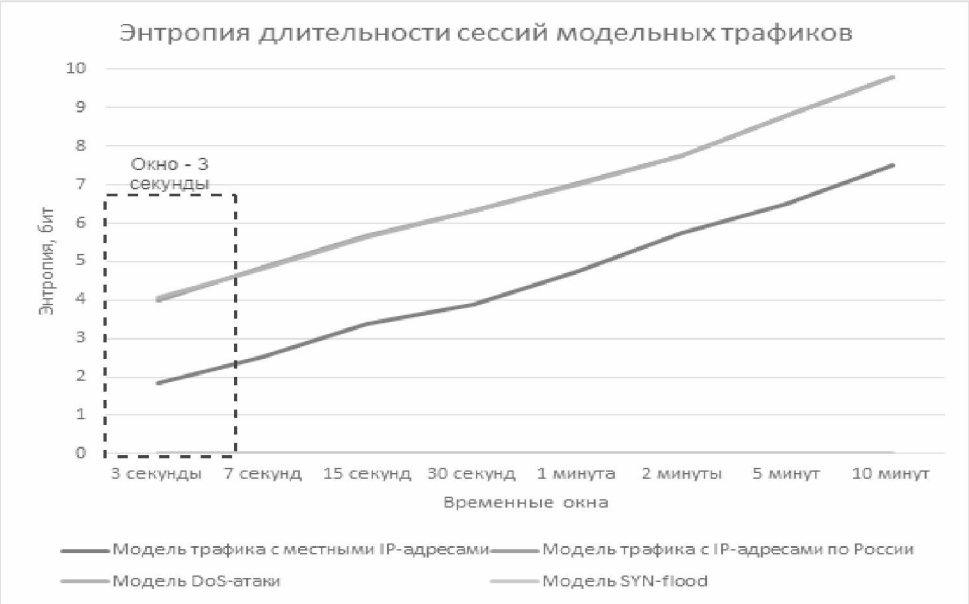

Рисунок 2 – График выбора временного окна у энтропии длительности модельных трафиков

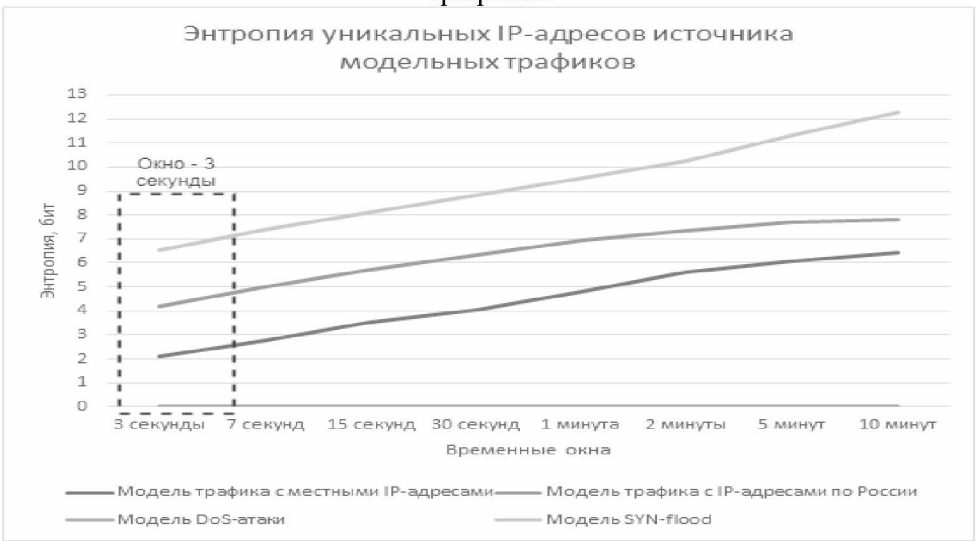

Рисунок 3 - График выбора временного окна у энтропии IP-адресов источника модельных трафиков

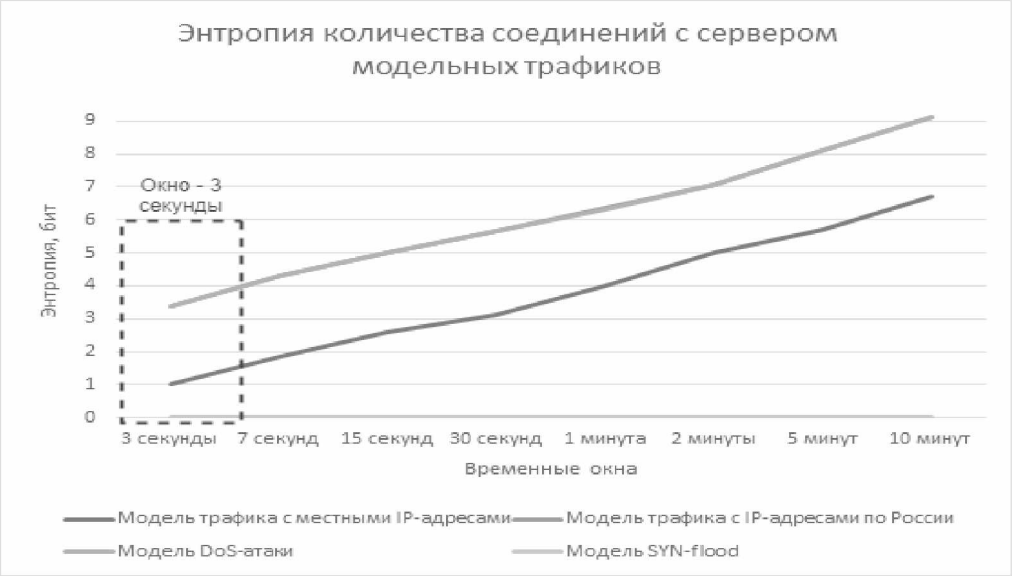

Рисунок 4 - График выбора временного окна у энтропии соединений с сервером модельных трафиков

В случаях, когда один трафик похож на другой, помогает характеристика среднего времени сессии, значения которой представлены на рисунке 5. Из анализа данного графика видно, что модели легитимных трафиков имеют достаточно большие значения, а аномальные трафики либо значения, не превышающие 1 секунду, для DoS-трафика, или значения, равные нулю, для SYN-flood атаки.

После анализа модельных трафиков исследуется реальный трафик. К реальному трафику добавляется BitTorrent трафик для проверки алгоритма на возможность отличать аномальный трафик от легитимного трафика.

Рисунки 6-8 демонстрируют, что выбранные характеристики позволяют корректно отделять трафик друг от друга уже на третьей секунды захвата трафика, из чего делается вывод о достаточности данного окна

Рисунок 5 – График среднего времени сессии для модельных трафиков в промежутке от 3 секунд до 10 минут.

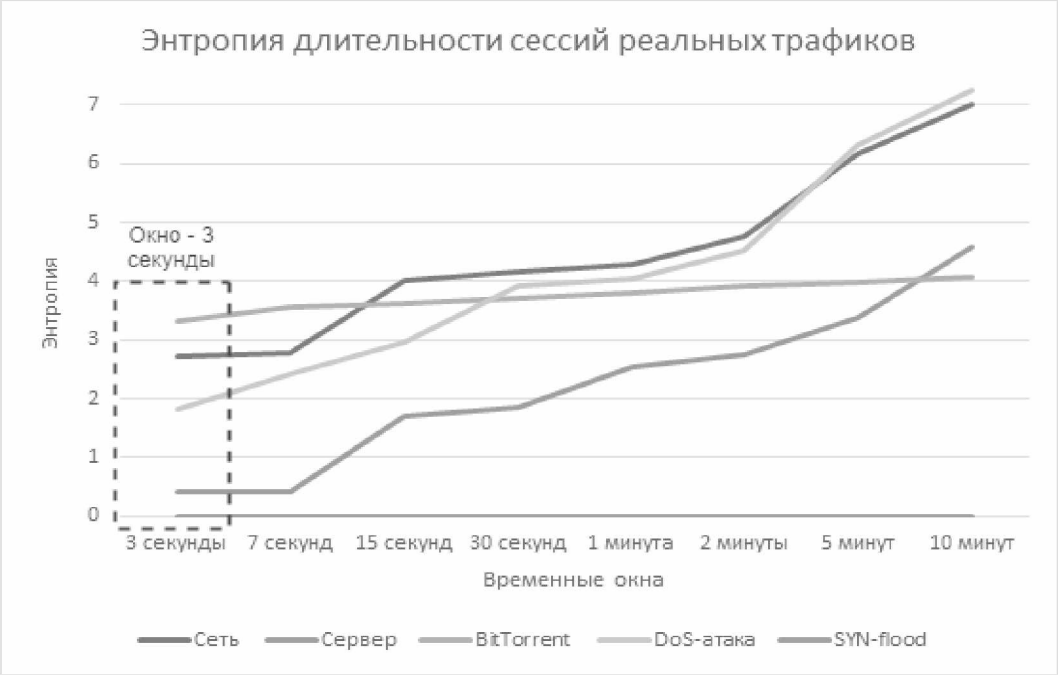

Рисунок 6 - График выбора временного окна у энтропии длительности сессий реальных трафиков

Анализ среднего времени сессии для реальных трафиков, представленный на рисунке 9, показывает, что, как и в предыдущем пункте, данная характеристика помогает с детектированием аномального трафика, поскольку значения этой характеристики для легитимных трафиков намного больше, чем ее значения для трафиков атак.

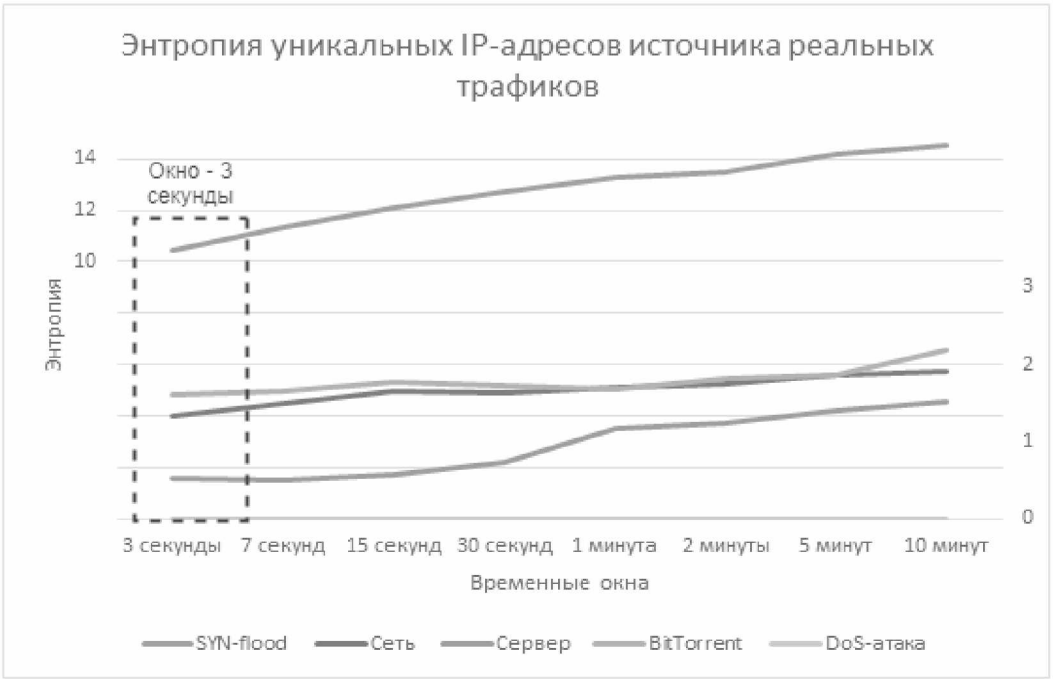

Рисунок 7 - График выбора временного окна у энтропии IP-адресов источника реальных трафиков

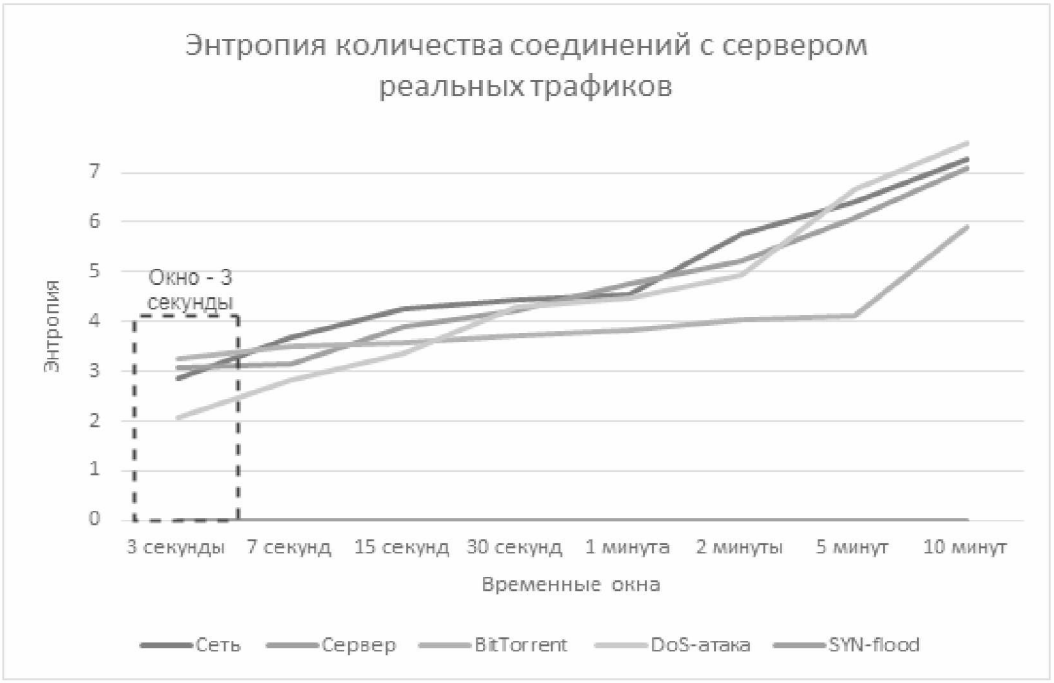

Рисунок 8 - График выбора временного окна у энтропии соединений с сервером реальных трафиков

Предлагаемый метод также проверен на комбинациях модельного и реального трафика. Рисунок 10 демонстрирует достаточность «окна» в 3 секунды для идентификации аномального трафика и возможности его отличать от легитимного. Рисунок 11 показывает, что характеристика энтропии длительности сессий наилучшим образом отличает SYN-flood атаку. Характеристика, представленная на рисунке 12, является чувствительной для разных видов трафика в окне 3 секунды.

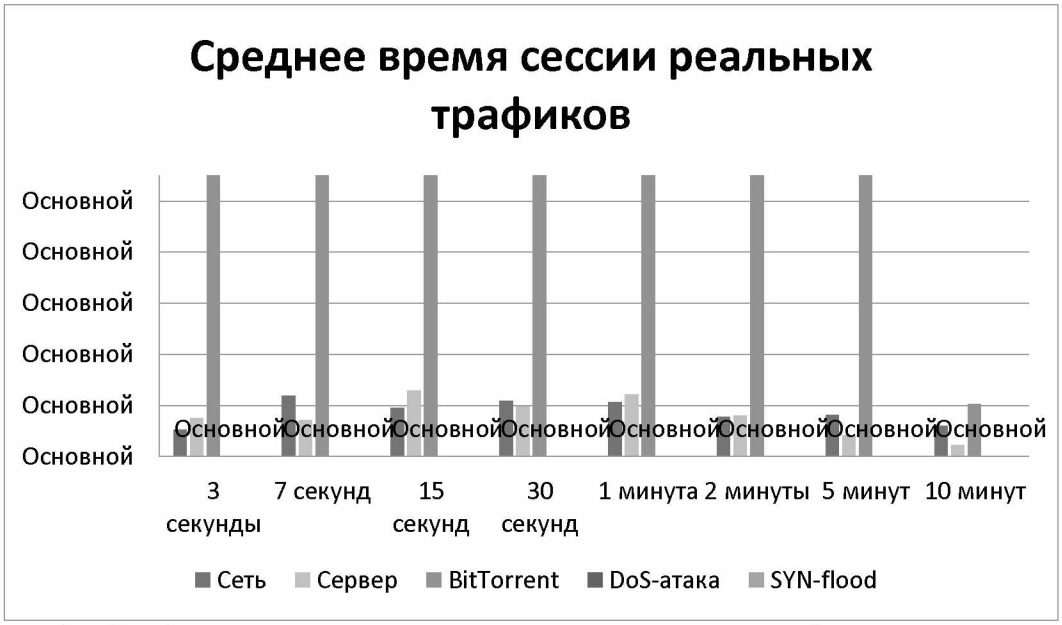

Рисунок 9 – График среднего времени сессии для реальных трафиков в промежутке от 3 секунд до 10 минут.

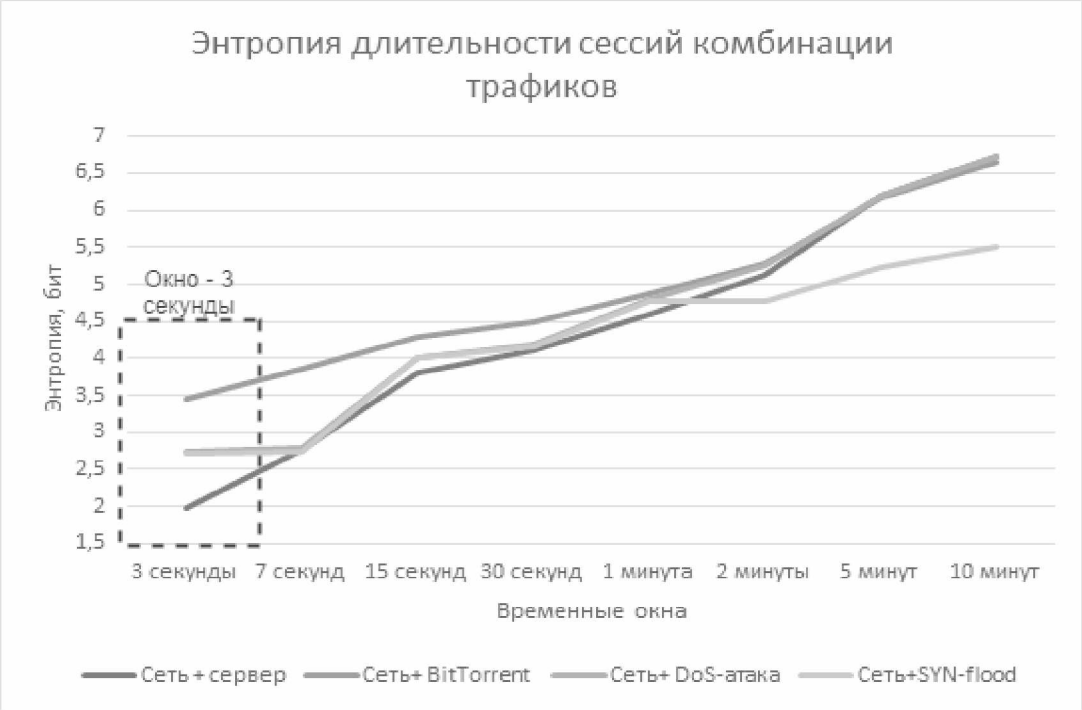

Рисунок 10 - График выбора временного окна у энтропии длительности сессий комбинации трафиков

В результате проведенного тестирования на 13 образцах сетевого трафика показана эффективность предлагаемого метода идентификации сетевых атак с использованием рабочего «окна» анализа в 3 секунды. Метод может определять наличие DoS/DDoS-атаки и вид самой атаки, начиная с трех секунд захвата сетевого трафика.

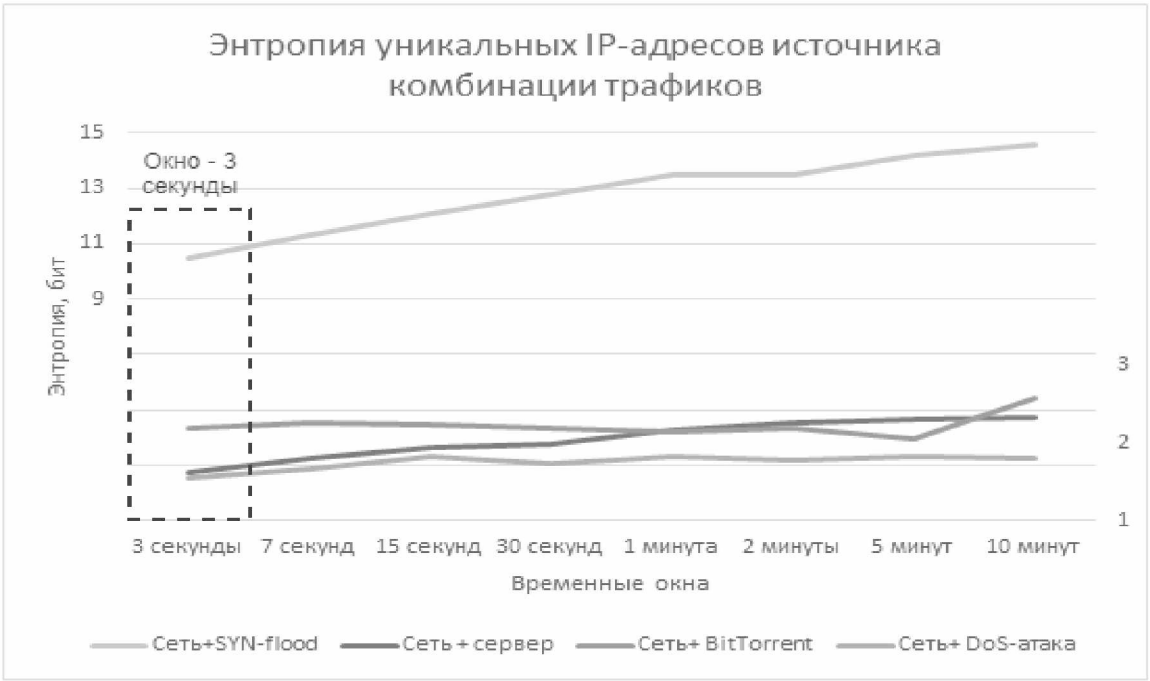

Рисунок 11 - График выбора временного окна у энтропии IP-адресов источника комбинации трафиков

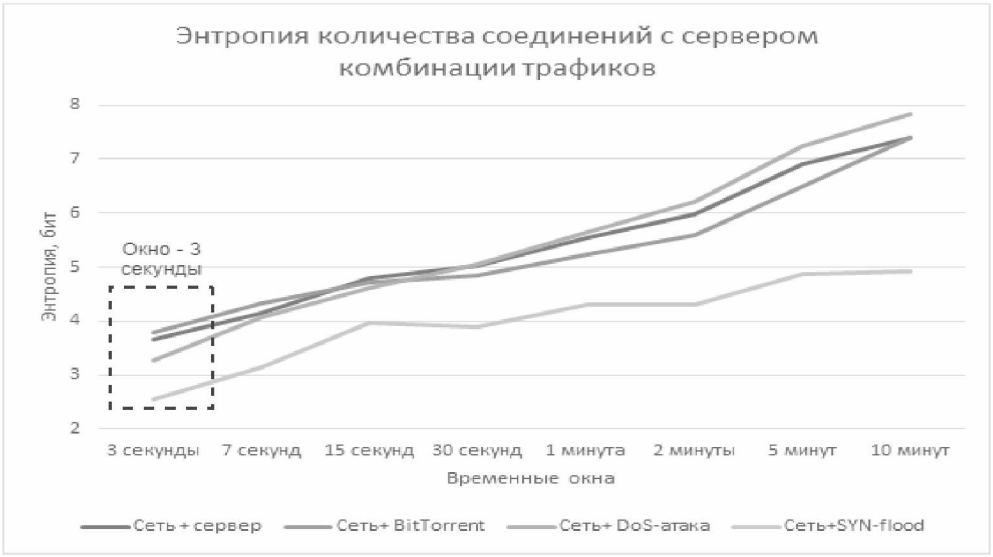

Рисунок 12 - График выбора временного окна у энтропии соединений с сервером комбинации трафиков

Библиографический список

1. Zekri M., Kafhali S., Aboutabit N., Saadi Y. DDoS Attack Detection using Machine Learning Techniques in Cloud Computing Environments // 3rd International Conference of Cloud Computing Technologies and Applications (CloudTech 2017). – 2017. – С.236 – 242.
2. Alzahrani, S., Hong, L. A Survey of Cloud Com- puting Detection Techniques against DDoS Attacks. Journal of Information Security, - 2018 - №9. С.45-69.
3. Zhijun Wu, Liyuan Zhang, Meng Yue. Rate DoS Attacks Detection Based on Network Multifractal // IEEE Transactions on Dependable and Secure Computing – 2018. - №13. – С.559 – 567.
4. Fractal Network Traffic Analysis with Applications [Электронный ресурс]. // URL: https://pdfs.semanticscholar.org/9fff/1ee5e97825b8971e1d5030bf8cd20ae89710.pdf.
5. Abry P., Baraniuk R., Flandrin P., Riedi R., Veitch D. Multiscale nature of network traffic // IEEE Signal Processing Magazine – 2002. – №19. – С.28–46.
6. Rajvir K., Gauravdeep. Statistical based DDoS Detection Methods: A Review. International Journal of Engineering Technology // Management and Applied Sciences. - 2017. - №5. – С.521 – 525.
7. Fang-Yie L., I-Long L. A DoS/DDoS Attack Detection System Using Chi-Square Statistic Approach. Systemics // Cybernetics and informatics. - 2010 – №8. – С.41 – 51.
8. Машинно-синестетический подход к обнаружению сетевых DDoS-атак [Электронный ресурс]. // URL: https://habr.com/ru/company/otus/blog/441182/
9. Шелухин О.И. Мультифракталы // Инфокоммуникационные приложения // М.: Горячая линия-Телеком. - 2011. – 576 С.
10. Обнаружение аномалий в информационных процессах на основе мультифрактального анализа [Электронный ресурс] // URL: https://cyberrus.com/wp-content/uploads/2015/01/vkb_05_04.pdf.
11. Detecting Distributed Denial of Service Attacks: Methods, Tools and Future Directions [Электронный ресурс]. // URL: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.469.4941&rep=rep1&type=pdf
12. Detection Techniques against DDoS Attacks: A Comprehensive Review [Электронный ресурс] // URL: https://pdfs.semanticscholar.org/f9a2/2ba17ec0313d96d0c54f4a047212c463bf6e.pdf