Д. П. Марцулевич
(*ГрГУ им. Я. Купалы, Гродно*)

ОБНАРУЖЕНИЕ DDOS АТАК НА УРОВНЕ ПРИЛОЖЕНИЯ ИСПОЛЬЗУЯ ОДНОКЛАССОВЫЙ МЕТОД ОПОРНЫХ ВЕКТОРОВ

Алгоритм, реализуемый в работе, основан на извлечении 7 основных признаков (общее количество запросов за сеанс, средняя вероятность перехода всех смежных запросов в сеансе, общий размер всех запросов в сеансе, продолжительность сеанса, код ответа, время загрузки динамических страниц, средняя популярность всех запросов в сеансе) из сеансов обычных пользователей и дальнейшем построении модели "настоящего" пользователя, которая используется для обнаружения аномального поведения, т.е. DDoS-атак (рис. 1).

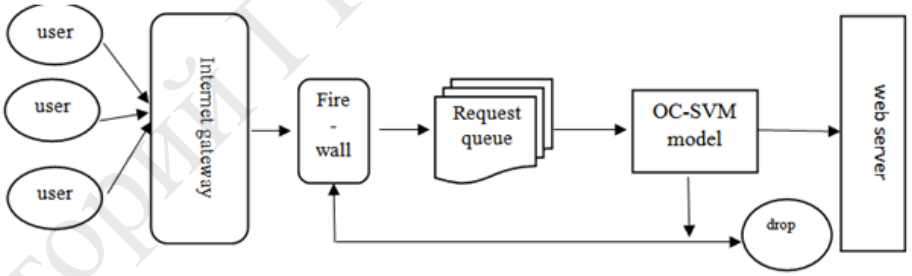

Рисунок 1 – Схема архитектуры обнаружения

Алгоритм процесса обнаружения на псевдокоде:

```
i = 0;
while i < sessions.size
    if f(x_i) returns -1 then normal = false;
    else if f(x_i) returns 1 then normal = true;
    endif;
    if normal == false then <discard current request and block this session[i].IP
and add this IP to blacklist>
    endif;
```

```
        i = i + 1;
    endwhile;
```

Численные результаты, основанные на имитационных экспериментах, демонстрируют эффективность данного метода обнаружения DDoS-атак.