УДК 004.724

ИССЛЕДОВАНИЕ И РАЗРАБОТКА АЛГОРИТМА ОБНАРУЖЕНИЯ И ПРЕДОТВРАЩЕНИЯ DDOS АТАК НА КОНТРОЛЛЕР В ПРОГРАММНО-КОНФИГУРИРУЕМЫХ СЕТЯХ

Д. Врублевский
(Санкт-Петербург, Университет ИТМО) **Научный руководитель – к.т.н., доцент кафедры СиОТ В.А. Грудинин** (Санкт-Петербург, Университет ИТМО)

Угроза DDoS является одной из основных атак, которой могут быть подвержены программно-конфигурируемые сети. Внедрение управляющего компонента сети – контроллера, закономерным образом приводит к появлению единого слабого места всей сети ПКС.

Опасность атак типа «отказ в обслуживании», следует из самого алгоритма работы ПКС-коммутатора. При приеме на вход неизвестного пакета, т. е. не соответствующего под внесенные правила в таблице потоков, коммутатор либо отправляет весь данный пакет на контроллер, либо отправляет на контроллер только заголовок пакета, при этом сохраняя сам пакет в памяти коммутатора.

Следовательно, в ходе проведения DDoS атак происходить переполнение канала связи между коммутаторами и контроллером, чрезмерная нагрузка на вычислительные ресурсы контроллера, увеличение используемой внутренней памяти коммутаторов.

В данной работе автором были исследованы методы обнаружения и предотвращения DDoS атак на контроллер в программно-конфигурируемых сетях. Был предложен свой алгоритм по противодействию данных тип атак, а также метод по уменьшению воздействия таких угроз на компоненты ПКС.

Целью работы является исследование и разработка эффективного метода выявления атак DDoS на контроллер ПКС на основе вероятностного изменения ip-адреса источника. Для выявления наличий аномалий применен метод энтропийного изменения сетевого взаимодействия, производится анализ параметров потока: ip-адрес назначения, ip-адрес источника. номеров портов и т.д.

В ходе работы были изучены архитектура SDN, этапы выполнения DDoS атак, выявлены последствия данных тип атак на элементы ПКС , проанализированы существующие алгоритмы по обнаружению DDoS угроз на программно-конфигурируемые сети.

Заключение. В результате проделанной работы автором был предложен алгоритм по раннему обнаружению и уменьшению воздействий DDoS атак на контроллер.

Автор _____ / Д. Врублевский/

Научный руководитель _____ / В.А. Грудинин/

Заведующий кафедрой СиОТ _____ / С. Э. Хоружников/