С. С. Бармина, *студентка, Казанский национальный исследовательский технический университет им. А. Н. Туполева – КАИ, molibdenbora@yandex.ru*

Ф. М. Таджибаева, *студентка, Казанский национальный исследовательский технический университет им. А. Н. Туполева – КАИ, frida.t.1465@gmail.com*

М. В. Тумбинская, *канд. техн. наук, Казанский национальный исследовательский технический университет им. А. Н. Туполева – КАИ, tumbinskaya@inbox.ru*

Корреляционный анализ и прогнозирование SYN-флуд атак

Веб-ресурсы являются неотъемлемой частью жизни современного человека. Так же, как и другие элементы IT-сферы, они подвержены хакерским атакам. Среди лидеров атак можно выделить внедрение операторов SQL и межсайтовое выполнение сценариев. Несмотря на это, DDoS-атаки продолжают входить в топ-10 сетевых атак и приводить к серьезным сбоям работы веб-ресурсов. В статье рассмотрены DDoS-атаки, их классификация и методы защиты. Особое внимание уделено наиболее распространенному типу DDoS-атак — SYN-флуд атакам, анализу их временно́го ряда и прогнозированию.

Ключевые слова: DDoS-атаки, SYN-флуд, прогнозирование, веб-ресурсы, защита информации.

Введение

DoS (Denial of Service) — хакерская атака на вычислительную систему с целью довести ее до отказа. DoS-атака представляет собой генерацию «мусорного» трафика с одного устройства (IP-адреса) на ресурс-жертву. Схема DoS — основа современных кибератак на отказ в обслуживании, при реализации которой не остается юридически значимых улик. DDoS-атаки являются подтипом DoS-атак и применяются там, где последние могут оказаться неэффективны. Атаки при этом осуществляются с нескольких компьютеров сети, которые объединяются, и каждый производит атаку на систему жертвы. Часто DDoS-атаки реализуют при помощи зараженных специальными программами компьютеров (ботнетов), которые часто называют «компьютерами-зомби».

Авторами работы [1] описывается инцидент, который принято считать первой в мире DDoS-атакой, — атака на IRC-сервер университета Миннесоты в 1999 г. Тогда сервер был выведен из строя на несколько дней. DDoS-атаки стали быстро распространяться, и уже к 2000 г. с их помощью была парализована работа компаний *eBay*, *Amazon*, *CNN*, *Yahoo*. Эти инциденты продемонстрировали эффективность атак типа «отказ в обслуживании», вследствие чего скорость DDoS-атак стала стремительно повышаться, а к 2010 г. они выросли до политического уровня. В этот год сайты мировых платежных систем *PayPal*, *Visa* и *Mastercard* были атакованы группой *Anonymous*.

Цель злоумышленников, использующих DDoS-атаки, согласно работе [2] чаще всего заключается в следующем: выразить свой протест политике страны или отдельной компании, тем самым заявив о себе. Однако часто такие атаки прикрывают реальные намерения злоумышленника. Это своего рода отвлекающий маневр: в то время как специалисты ресурса-жертвы пытаются отразить атаку и восстановить нормальную работу сервиса, на самом деле злоумышленники похищают