DOI: 10.37791/2687-0649-2020-15-5-85-102

Использование статистических методов для анализа и прогноза udp-flood атак

М. В. Тумбинская[1*]***, В. В. Волкова***[1]***, Б. Г. Загидуллин***[1]
[1] *Казанский национальный исследовательский технический университет им. А. Н. Туполева, г. Казань, Россия*
** tumbinskaya@inbox.ru*

Аннотация. Web-ресурсы являются неотъемлемой частью жизни современного человека, которые в настоящее время все чаще подвергаются хакерским атакам, таким как внедрение операторов SQL, межсайтовое выполнение сценариев и др. DDoS-атаки продолжают входить в топ-10 сетевых атак и приводить к серьезным сбоям и отказам работы web--ресурсов, наиболее распространенным типом DDoS-атак является UDP-flood атаки, основанные на бесконечной посылке UDP-пакетов на порты различных UDP-сервисов. Основанием для проведения эмпирического исследования являются факторы: отсутствие эффективных средств защиты от DDoS-атак, специфика UDP-flood атак, отсутствие моделей прогнозирования, адекватно описывающих исследуемый процесс. Целью исследования является повышение уровня защищённости web-ресурсов, за счет своевременного обнаружения аномалий в их работе, обнаружении информационных угроз безопасности на основе методов анализа и прогнозирования. В качестве объекта исследования был выбран тип атак UDP-flood из семейства DDoS атак. Методами корреляционного анализа и моделирования были рассчитаны индекс сезонности UDP-flood атак, автокорреляция временного ряда данного типа атак, на основе моделей простого экспоненциального сглаживания и нейросетевого прогнозирования построен прогноз UDP-flood атак. В работе предложена классификация DDoS-атак, описаны способы защиты. На основе корреляционного анализа рассчитаны прогнозные значения воздействия UDP-flood атак на web-ресурсы, выявлен фактор – сезонность. Анализ результатов прогнозирования показал, что разброс прогнозных значений не значительный, наибольшее количество атак ожидается в IV квартале 2020 года. Для DDoS-атак длительностью до 20 минут также выявлена сезонность в I квартале календарного года, а значит, в I квартале 2020 года следует ожидать наибольшее количество атак данной длительности. Перспективы дальнейшего исследования проблемы защиты от DDoS атак представляются в дальнейшей проработке методики противодействия UDP-flood атакам, алгоритмов информационной безопасности web-ресурсов, что позволит сократить количество инцидентов UDP-flood атак, планировать мероприятия по повышению уровня защищенности web-ресурсов, повысить уровень их защищенности.

Ключевые слова: DDoS-атака, UDP-flood, корреляционный анализ, прогнозирование, метод простого экспоненциального сглаживания, коэффициент сглаживания, моделирование, аддитивная модель временных рядов, автокорреляционная функция, защита информации

Для цитирования: *Тумбинская М. В., Волков В. В., Загидуллин Б. Г.* Использование статистических методов для анализа и прогноза UDP-flood атак // Прикладная информатика. 2020. Т.15 № 5. С. 85–102. DOI: 10.37791/2687-0649-2020-15-5-85-102