ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ УНИВЕРСИТЕТА

Е.И. Шаронова, С.И. Матюшкин

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь

Университетские информационные системы являются ключевой составляющей инфраструктуры университетов, которые поддерживают учебный процесс, административные функции и другие виды деятельности. Поэтому обеспечение доступности университетских информационных систем является критически важным, чтобы обеспечить непрерывность работы университета. Соответственно, важнейшей задачей становится обеспечение доступности информационных сервисов университета.

Распространенными практиками по обеспечения доступности являются: резервное копирование; обнаружение сбоев; балансировка нагрузки; резервирование и зеркальных серверов.

DDoS является угрозой для бесперебойной работы информационных сервисов, последствия от которой бывают как технические, финансовые, так и репутационные. Для генерации трафика злоумышленники используют различные источники: обычные компьютеры и серверы; умные устройства Интернета-вещей; сетевые устройства; рекламные сервисы.

Машинное обучение является набирающим популярность направлением, применяется оно и для обнаружения DDoS-атак. Существует множество продуктов, включая облачные решения, которые используют машинное обучение для обнаружения DDoS-атак путем анализа сетевого трафика и выявления аномалий. Например, Radware DefensePro, F5 Silverline DDoS Protection, Arbor Networks Peakflow, Imperva Incapsula, Neustar SiteProtect и т.п. Эти решения использует алгоритмы машинного обучения.

Нейронные сети используются для обработки больших объемов данных и обучения моделей, которые могут определять характерные признаки ботнетов. Примерами таких проектов являются Deep Defense, Botwall, Botnet Detection Based on Deep Learning, BotMine. Эти модели анализирует трафик и идентифицирует характеристики ботнетов, такие как IP-адреса и сигнатуры вредоносных программ, скорость сетевого трафика и длительность соединения.

Соответственно, перспективным является внедрение решений на основе машинного обучения для обеспечения защиты интегрированной информационной системы Белорусского государственного университета информатики и радиоэлектроники с учетом состояния современного рынка средств защиты от DDoS атак.