ОБНАРУЖЕНИЕ ИНФОРМАЦИОННЫХ УГРОЗ БЕЗОПАСНОСТИ ПЕРЕДАЧИ ДАННЫХ В ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЯХ

А.В. Гирик
Санкт-Петербургский государственный университет информационных технологий, механики и оптики
Тел.: (812) 595-41-32, e-mail: c0mplex@land.ru

Исследование и разработка моделей и методов информационного противодействия угрозам нарушения информационной безопасности является актуальной задачей как для ЛВС, так и для открытых глобальных сетей. Одной из составляющих процесса оценки устойчивости работы сети является обнаружение аномалий в работе сети как отклонений от нормального поведения трафика. Какие явления можно отнести к числу сетевых аномалий? В первую очередь это:

1. Нештатные ситуации в работе сети:
- сбои в работе или выход из строя сетевых устройств;
- изменения конфигурации сетевых устройств или сети в целом (например, применение новых граничных значений для шейпера).

2. Перегрузки:
- так называемые flash crowds (или slashdot effects);
- широковещательные штормы в ЛВС.

3. Атаки:
- типа «отказ в обслуживании» (*Denial of Service*, *DoS*);
- сканирование портов;
- другие типы атак.

Мониторинг состояния сети передачи данных (СПД), находящейся под воздействием угроз нарушения целостности, и сравнение фактических результатов с прогнозными позволяет обнаруживать сетевые аномалии и более точно идентифицировать их характер и источник. Таким образом, к основным компонентам модели обнаружения угроз безопасности в СПД можно отнести:

- Мониторинг показателей функционирования.
- Прогнозирование показателей функционирования.
- Обнаружение и идентификация угроз.

Рассмотрим более подробно каждый из компонентов этой модели. Мониторинг СПД может осуществляться различными способами в зависимости от параметров и характеристик сети, уровня безопасности, который необходимо обеспечить и т.д. К основным методам мониторинга сети в целом можно отнести:

- Мониторинг на основе SNMP.
- Мониторинг потоков данных (NetFlow, JFlow, NetStream, sFlow).
- Анализ сетевых пакетов.
- Трассировка событий сетевого стека (например, с помощью DTrace).
- Сквозной мониторинг (на основе ICMP, UDP, TCP).
- Инструментирование приложений.
- Анализ журналов прикладных и системных программ.

Мониторинг СПД необходим для того, чтобы можно было сформировать *нормальный профиль* работы сети, исходя из которого будет формироваться прогноз и оцениваться расхождение реальных значений показателей с прогнозными. Существует большое количество методов прогнозирования процессов, протекающих в СПД, к основным можно отнести:

- Использование марковских моделей.
- Имитационное моделирование.
- Фрактальные броуновские процессы.
- Анализ временных рядов.

Построение прогнозов на основе анализа временных рядов получило значительное распространение в эконометрике и впоследствии стало использоваться и для моделирования поведения процессов в сетях передачи данных. В общем случае временной ряд может быть представлен мультипликативной моделью вида

$$X(t) = T(t) \cdot C(t) \cdot S(t) \cdot \varepsilon(t),$$

где $T(t)$ – основная закономерность развития процесса во времени, или тренд, $C(t)$ – циклическая составляющая, $S(t)$ – сезонная составляющая, $\varepsilon(t)$ – случайные колебания. В зависимости от природы процесса, порождающего ряд, и длительности наблюдений те или иные составляющие ряда могут отсутствовать. Удобно представлять ряд в виде совокупности процессов авторегрессии – скользящего

среднего (АРСС) или – для нестационарных процессов – процессом, приращения которого могут быть описаны моделью АРСС.

Экспериментальные данные показывают, что в большинстве случаев трафик в сети обнаруживает периодические колебания. Анализ автокоррелограммы позволяет выявить сезонные эффекты с периодом 1 час, 24 часа (сутки) и 168 часов (неделя). Для учета периодичностей и процессов, которые невозможно выявить с помощью анализа автокорреляционной функции ряда, предлагается использовать метод аналогий, или метод ретроспективного поиска.

Другой подход заключается в том, чтобы рассматривать ряд как совокупность тренда, колебаний и случайных флуктуаций, причем моделирование тренда выполнять с помощью регрессионного анализа, периодическую составляющую описывать рядом Фурье и использовать методы и средства анализа периодограмм и спектрального анализа случайных процессов. Этот подход к анализу временных рядов и построению прогнозов можно считать классическим.

После того, как сформирован прогноз, необходимо сравнить прогноз с реальными значениями показателей, и, учитывая возможные ошибки, принять решение о том, насколько значительно отличается поведение показателей от ранее сформированного нормального профиля. В случае, если это расхождение признается превосходящим возможные погрешности прогноза, имеет место аномалия в поведении некоторого показателя, что в свою очередь может являться признаком сетевой атаки или неисправности оборудования или программных средств.

Описанная модель находит применение в системах защиты от вторжений в сеть (*Network Intrusion Detection System*). В общем случае угрозу нужно сначала обнаружить, а затем идентифицировать. Как правило, для идентификации угрозы необходимо больше информации, чем для её обнаружения, но более информативный мониторинг создает бо́льшую нагрузку на сеть и приводит к потерям производительности. Поэтому целесообразно задействовать механизмы подробного анализа после обнаружения угрозы. Рассмотренные принципы обнаружения информационных угроз передачи данных с СПД были применены при проектировании системы управления сетью одного из петербургских провайдеров (UNIS, http://www.unisnet.ru).