УДК 004.056.5 + 519.242.7

МАТЕМАТИЧЕСКАЯ МОДЕЛЬ И ЭКСПЕРИМЕНТАЛЬНОЕ ИССЛЕДОВАНИЕ ХАРАКТЕРИСТИК МЕЖСЕТЕВОГО ЭКРАНА

Студент Муллин А.Р.
Канд. техн. наук, доцент Быков А.Ю.
МГТУ имени Н.Э. Баумана

При разработке стека TCP/IP – основы сети Интернет – не было уделено должного внимания вопросам безопасности. В результате в мире Интернет до сих пор остро стоят вопросы информационной безопасности. Одним из методов защиты сетевых информационных ресурсов организации является использование специальных программных (программно-аппаратных) средств, называемых в англоязычной литературе FireWall (огненная стена). В отечественной технической литературе их принято называть межсетевыми экранами (МЭ) [1].

Межсетевой экран в современном понимании представляет собой многофункциональное и многокомпонентное устройство, то есть систему. Для научного исследования системы мы прибегаем к определенным допущениям, касающимся ее функционирования. Эти допущения, как правило, имеющие вид математических или логических отношений, составляют модель, с помощью которой можно получить представление о поведении соответствующей системы [2].

В эксперименте будем моделировать работу МЭ, в частности, алгоритмы фильтрации по разным признакам. Суть эксперимента заключается в следующем - мы генерируем 1000 пакетов типа TCP и посылаем их в сеть, при этом в трафик намеренно включаем незаконные пакеты. С помощью программы Sniffer Win мы в командной строке видим пройденные в сеть пакеты, в этой же программе будем моделировать фильтрацию пакетов.

Авторами была разработана программа, которая генерирует пакеты TCP. Также были произведены эксперименты и построена математическая модель эксперимента, а также рассчитаны главные эффекты двух факторов.

Эксперименты показали, что фактор — фильтрация по IP-адресам имеет немного большую по модулю значимость, чем фактор — фильтрация по номерам портов. Построенная модель в дальнейшем может быть усовершенствована путем введения в нее дополнительных факторов фильтрации.

Литература

1. Лебедь С.В. Межсетевое экранирование. Теория и практика защиты внешнего периметра. – М.: Изд-во МГТУ им. Н.Э Баумана, 2002. – 304 с.: ил.

2. Кельтон В., Лоу А. Имитационное моделирование. Классика CS 3-е изд. – СПб.: Питер; Киев: Издательская группа BHV, 2004 – 847 с

УДК 681

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ (ИБ) В МОБИЛЬНЫХ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМАХ (ИТКС)

Магистрант Коростелев В.К.
Канд. техн. наук, доцент Медведев Н.В.
МГТУ имени Н.Э. Баумана

Целью исследования является снижение рисков нарушения ИБ в ИТКС использующих технологию облачных вычислений при обработке информации различной степени конфиденциальности в операционных средах типа Android. Для решения проблемы предложен метод анализа данных на основе учета параметров уровня защищенности ресурсов облачной ИТКС.

Использование Байесовского подхода для анализа потенциальных угроз ИТКС, основанных на использовании операционных сред типа Android, даст возможность осуществить выявление зависимости между факторами влияющими на ИБ;

В случае анализа уровня защищенности ресурсов ИТКС рассматривается случайная величина Y, которая имеет плотность вероятности с параметрами δ. На основании полученных статистических данных можно сделать вывод о другой случайной величине δ, имеющей распределение вероятности $\pi(\delta)$. Тогда согласно формуле Байеса

$$p(\delta \mid y) = \frac{p(y \mid \delta)P(\delta)}{p(y)}$$

Основными признаками защищенности ресурсов облачной ИТКС служит следующий кортеж показателей: способность обеспечить конфиденциальность (C), целостность (N) и доступность (M) информации при воздействии угроз определенного типа.

Если одновременно получены три показателя, то в соответствии с теоремой Байеса, используется формула

$$P(\delta_i/C,N,M) = \frac{P(C/\delta_i)P(N/\delta_i)P(M/\delta_i)P(\delta_i)}{\sum_{i=1}^{3} P(C/\delta_i)P(N/\delta_i)P(M/\delta_i)P(\delta_i)}$$

Если в результате исследования выяснилось, что СЗИ не обеспечила кортеж показателей защищенности информации при воздействии угрозы, то необходимо рассматривать противоположные события:

$$P(\overline{CNM}/\delta_i) = 1 - P(C,N,M/\delta_i).$$