М. Б. Карюкова, **Р. Н. Селин**, **С. А. Чурилов** (Ростов-на-Дону, ФГНУ НИИ «Спецвузавтоматика»)**. Обнаружение каналов утечек информации в корпоративной сети, использующих протокол HTTP.**

В докладе рассматриваются вопросы защиты информации, обрабатываемой в корпоративных сетях, в тех случаях, когда нарушитель находится внутри корпоративной сети. В таких случаях обычно злоумышленник или вредоносное ПО пытается передать данные за пределы защищенного сетевого периметра. Одним из каналов утечки в таком случае может являться http-трафик организации, если корпоративная политика безопасности допускает работу пользователей в Интернет.

Распространенным методом является туннелирование недопустимых сетевых протоколов через разрешенные либо маскировка под имеющиеся допустимые программные средства.

Согласно спецификации протокола http, каждое http-сообщение состоит из трех частей. Указанные части передаются в следующем порядке: стартовая строка, заголовки, тело сообщения. Будем анализировать различные части сессии http-сообщения.

Оценку принадлежности φ http-сообщения (сессии) к каналу утечки информации построим на основе многокритериальной оценки по ряду экспертных признаков, формируемых на этапе обучения модели. Для этого производился анализ четырех видов трафика. Первый вид трафика — это трафик, принадлежащий каналу утечки информации через туннель HTTP. Второй, третий и четвертый виды трафика — это легальный трафик, принадлежащий наиболее распространенным браузерам: Microsoft Internet Explorer, Mozilla Firefox, Opera соответственно. Были отобраны следующие критерии.

Для запросов http: k_1 — версия протокола соответствует шаблону «HTTP/1.1»; k_2 — адрес соответствует шаблону вида «[text()][.php?/.asp?/.pl?] [text()]»; k_3 — адрес содержит малое количество гласных букв; k_4 — в строке адреса наблюдается постоянная смена регистра букв; k_5 — в адресе имеются хаотично разбросанные цифры; k_6 — в строке адреса отсутствует шаблон «html/htm»; k_7 — в строке адреса отсутствует шаблон «http://»; k_8 — в стартовой строке присутствует шаблон «GET»; k_9 — адрес превышает среднестатистическую длину; k_{10} — в заголовках присутствуют шаблоны, не соответствующие шаблонам стандартных браузеров; k_{11} — отсутствуют совпадающие подстроки между строкой адреса и значением заголовка «referer».

Для ответов http: k_{12} — в стартовой строке присутствует шаблон, отвечающий туннелированному трафику «HTTP/1.1 200 OK»; k_{13} — в заголовках присутствует шаблон, соответствующий туннелированному трафику.

Критерий принимает значение, равное 1, если соответствующее ему высказывание является истинным, и 0, если высказывание является ложным. Оценку построим в предположении равновесности всех указанных критериев $\varphi = \sum_{i=1}^{n} k_i$ [1].

СПИСОК ЛИТЕРАТУРЫ

1. *Горелик А. Л.*, *Скрипкин В. А.* Методы распознавания. М.: Высшая школа, 2004, 261 с.