УДК 004.7.052:004.414.2

Амирханов Э.Д., *аспирант*

СТАТИСТИЧЕСКИЙ АНАЛИЗ АНОМАЛИЙ В ГЕТЕРОГЕННЫХ СЕТЯХ ПО ИНФОРМАЦИОННОМУ КРИТЕРИЮ ФИШЕРА

Амірханов Е. Д. Статистичний аналіз аномалій в гетерогенних мережах по інформаційному критерію Фішера. Розглядається задача побудови інформаційної матриці Фішера при виявленні аномальної поведінки гетерогенних мереж. Розроблений комбінований метод виявлення аномалій, де у якості апріорних даних використовуються результати детермінованого аналізу сигнатур і протоколів вхідного потоку трафіку. Виведені вирази для асимптотично оптимальних оцінок параметрів вхідного потоку.

Ключові слова: МЕРЕЖНА АНОМАЛІЯ, ІНФОРМАЦІЙНА МАТРИЦЯ ФІШЕРА, НАПІВМАРКІВСЬКИЙ ПРОЦЕС, СИГНАТУРА, ПРОТОКОЛ

Амирханов Э. Д. Статистический анализ аномалий в гетерогенных сетях по информационному критерию Фишера. Рассматривается задача построения информационной матрицы Фишера при обнаружении аномального поведения гетерогенных сетей. Разработан комбинированный метод обнаружения аномалий, где в качестве априорных данных используются результаты детерминированного анализа сигнатур и/или протоколов входного потока трафика. Выведены выражения для асимптотически оптимальных оценок параметров входного потока.

Ключевые слова: СЕТЕВАЯ АНОМАЛИЯ, ИНФОРМАЦИОННАЯ МАТРИЦА ФИШЕРА, ПОЛУМАРКОВСКИЙ ПРОЦЕСС, СИГНАТУРА, ПРОТОКОЛ

Amirkhanov E. D. Statistical analysis of anomalies in heterogeneous networks on the Fisher information criterion. The task of construction of Fisher's information matrix is considered while abnormal behavior of heterogeneous computer networks is detecting. The combined method of anomalies detection is developed, where the results of the determined analysis of signatures and/or protocols of input streams of traffic uses as a priori information. The expressions for the asymptotically optimum estimates of parameters of input stream are deduced.

Keywords: NETWORK ANOMALY, FISHER INFORMATION MATRIX, SEMI-MARKOV PROCESS, SIGNATURE, PROTOCOL

Введение. Современные крупные информационно-вычислительные системы являются гетерогенными по определению [1, 2]. Неоднородность или гетерогенность присуща практически любым современным составным вычислительным и телекоммуникационным сетям. Эксплуатационно-технические характеристики отдельных сегментов, входящих в состав сети, могут значительно отличаться друг от друга. Например, пропускная способность одного сегмента может на порядок и более превышать пропускную способность другого сегмента. Такой разброс параметров приводит к существенному дисбалансу нагрузки на отдельные сегменты и маршруты передачи, нерациональному использованию ресурсов сети.

В корпоративной сети, в отличие от сети мегаполиса, число пользователей и число разновидностей подсетей меньше. В то же время в сети крупной производственной организации могут присутствовать самые разные типы вычислительных и телекоммуникационных сетей, вплоть до сенсорных и транкинговых.

На рис. 1 изображена гипотетическая схема корпоративной сети (КрС), связанной по различным линиям передачи данных (ЛПД) с терминальными узлами (ТУ). К терминальным узлам можно отнести автономные (по территориальному расположению) отделения и филиалы. Связь ТУ с КрС осуществляется провайдерами телекоммуникаций (ТЛК) и провайдерами Интернет.

Помимо дисбаланса нагрузки и нерационального использования располагаемых ресурсов, в гетерогенных сетях с различными физическими каналами передачи обостряются проблемы защиты от несанкционированного доступа, в первую очередь – от атак и вторжений. Не вдаваясь в причины роста злонамеренной сетевой активности, рассмотрим в данной работе задачи защиты от вторжений в вычислительные сети, т.е. внешние угрозы. Внутренние угрозы, конечно, также весьма распространены и опасны. По данным института компьютерной безопасности (*CSI*) в Сан-Франциско [3], от 60% до 80% неправомерной сетевой активности исходит от самих предприятий – пресловутый принцип Парето 20/80. В связи с этим для объективного анализа внешних угроз необходимо учитывать их корреляцию

с внутренними угрозами. Эта корреляция зависит от изменения степени уязвимости сети к внешним угрозам при возникновении внутренних угроз.

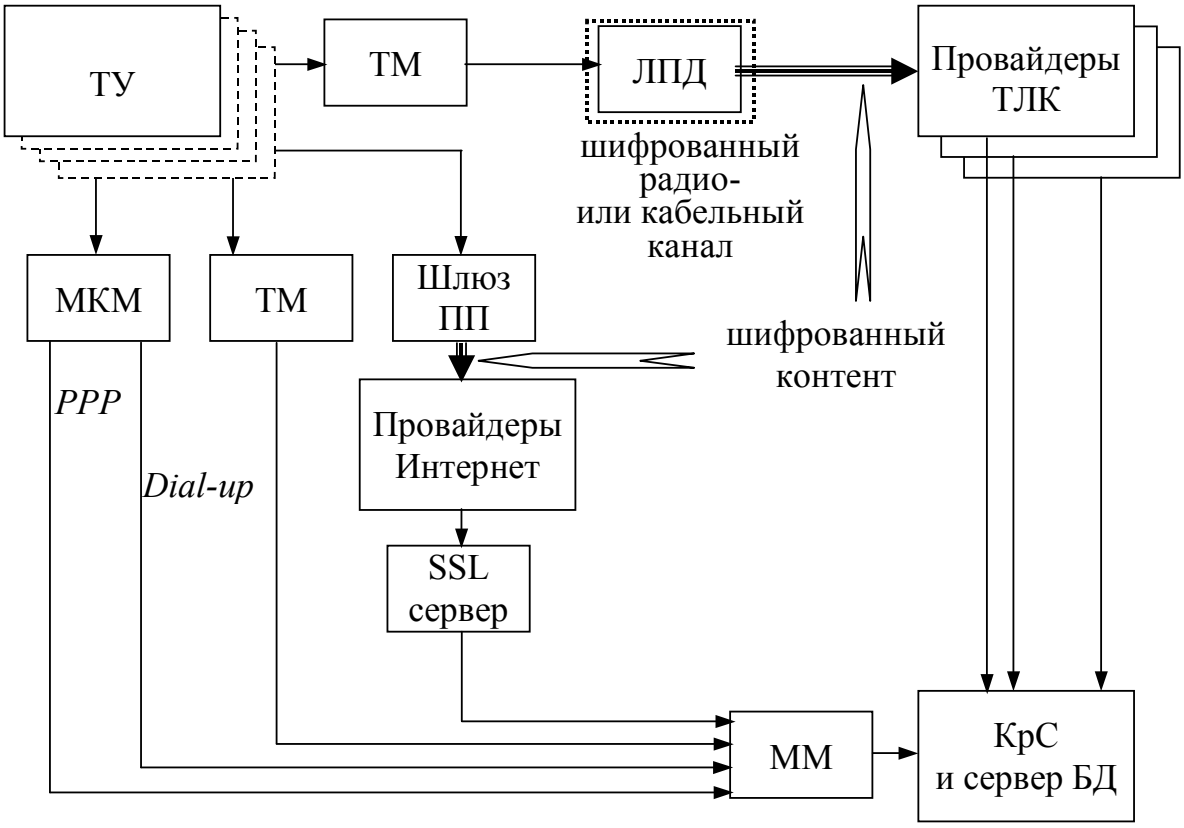

Рис. 1. Структура корпоративной сети

ТМ – терминальный маршрутизатор; МКМ – многоканальный модем; ММ – магистральный маршрутизатор; *PPP*, *Dial-Up* – протоколы передачи; БД – база данных; Шлюз ПП – шлюз пакетной передачи данных по протоколам *GPRS*/*EDGE*/3*G*.

Здесь рассматриваются статистические методы обнаружения аномалий в работе сети. В популярных статьях по системам обнаружения вторжений приводится много общих рассуждений о достоинствах и недостатках детерминированных и статистических подходов (см., напр., [4, 5 и др.]). Однако строгая постановка задачи статистического анализа и, тем более, ее решение методами теории проверки статистических гипотез в доступных нам источниках не встречаются. В данной работе сделана попытка восполнить этот пробел.

Постановка задачи. С датчиков системы обнаружения аномалий снимается информация о характеристиках трафика (выборка данных), которая анализируется для выявления аномального поведения, предшествующего атаке. Выборка данных на интервале наблюдения представляет собой совокупность реализаций – результатов оценивания параметров и состояния системы: *аномальные задержки* обмена между двумя пользователями; *многократные повторы* пакетов данных или служебных пакетов; *аномальная активность* устройств ввода-вывода; *аномальное число* нарушений памяти и пр.

Некоторые аномалии могут выявляться методами анализа детерминированных параметров (сигнатур или протоколов). В тех случаях, когда сигнатура (протокол) представляет собой ненормативное событие, например, вследствие намеренной модификации, детерминированный анализ не дает результатов. Кроме того, если между разными аномалиями имеется корреляция, одна аномалия может приводить к аномальному поведению с признаками другой аномалии. Поэтому необходимо обнаруживать аномалии методами теории проверки статистических гипотез.

По каждому элементу выборки проводится проверка простой гипотезы против простой альтернативы: результат измерения обычный – результат измерения аномальный. По

количеству обычных и аномальных результатов принимается общее решение о наличии или отсутствии попытки вторжения.

Для решения данной задачи необходимо: разработать *математическую модель* процесса обнаружения аномалий; выбрать *метод проверки* гипотез; выбрать *тип оценки* и вид функции потерь; разработать *метод выбора* оптимальных порогов обнаружения; разработать *метод расчета* статистических характеристик обнаружения.

В источниках теоретического и прикладного характера обоснованные рекомендации по выбору порогов отсутствуют. В практических разработках обычно используют разные средства регулировки порогов: от ручных до автоматизированных или полностью автоматических (адаптивных). Эта задача не является сугубо технической, поскольку присутствует человеческий фактор: при завышенных вероятностях обнаружения сигнала (низкий порог обнаружения) соответственно повышается частота ложных тревог, которая приводит к быстрой усталости оператора – администратора сети или менеджера по сетевой безопасности. Более того, он может просто перестать обращать внимание на некоторые сигналы, считая их ложными. Возникает риск пропуска угрозы. При снижении ложной тревоги (высокий порог обнаружения) естественно, падает и вероятность правильного обнаружения. Риск пропуска угрозы также растет, но уже по техническим причинам.

Поэтому можно предложить простой, но достаточно эффективный метод регулировки порога. Подсчитывается число ложных тревог за определенный временной интервал. Порог увеличивается или уменьшается, чтобы довести это число до величины, установленной на основе многократных наблюдений. В работах по инженерной психологии и эргономике [6,7] установлено, что при работе операторов систем наблюдения и обнаружения ложная тревога может иметь место в среднем не чаще, чем один раз за полчаса. При таких условиях оператор успевает возобновлять свое физическое и психологическое состояние. Реализация такого алгоритма в виде программы-модуля, включаемого в состав общего алгоритма обнаружения /оценивания, не представляет принципиальных трудностей.

Математическая модель процесса обнаружения аномалий. Процесс возникновения аномалии вследствие несанкционированной сетевой активности субъекта и процесс обнаружения рассматриваются как марковский процесс восстановления [8] одного из следующих типов:

- аномалия ϕ_2 – обнаружение ϕ_3; (1)
- аномалия ϕ_2 – обнаружение ϕ_3 – распознавание ϕ_4; (2)
- предотвращение аномалии ϕ_1 – аномалия ϕ_2 – обнаружение ϕ_3; (3)
- предотвращение аномалии ϕ_1 – аномалия ϕ_2 – обнаружение ϕ_3 – распознавание ϕ_4; (4)
- предотвращение аномалии ϕ_1 – аномалия ϕ_2 – обнаружение ϕ_3 – распознавание ϕ_4 – прогноз ϕ_5. (5)

Во всех случаях процессы имеют дискретный характер, переходы из произвольного состояния j в любое другое состояние k, $j,k=\overline{1,5}$, происходят скачком, а вероятности состояний меняются в зависимости от наличия априорной информации и вновь поступающей (апостериорной) информации. Отметим, что задача в такой постановке перекликается с задачами распознавания образов [9] или с задачами последовательного анализа [10].

Процессы вида (1…5), по существу, представляют собой дискретные полумарковские процессы с произвольным распределением времени t_i перехода в новое состояние ϕ_k. При заданном начальном состоянии $\{\phi_{0i}\}$, $i=\overline{1,5}$ развитие процесса полностью определяется матрицей вероятностей перехода $\{\rho_{jk}\}$, $j,k=\overline{1,5}$, и матрицей функций распределений $\{F_{jk}(t_i)\}$.

Наблюдаемый полумарковский процесс характеризуется финальными (при $t \to \infty$) вероятностями состояний p_j, которые не зависят от начального состояния и поэтому являются безусловными. Эти финальные вероятности являются решением системы алгебраических уравнений вида

$$p_j = \sum_{i=1}^{5} p_i \rho_{ij}, \quad \sum_{i=1}^{5} p_i = 1, \quad j = \overline{1,5}. \tag{6}$$

С учетом условия нормировки финальных вероятностей можно записать

$$\Xi_{ij} = p_j \left\langle T_j \right\rangle \left[\sum_{i=1}^{5} p_j \left\langle T_j \right\rangle \right]^{-1} = \Xi_j, \tag{7}$$

где $\left\langle T_j \right\rangle$ – средние безусловные интервалы ожидания в каждом из состояний (1…5).

Вероятностная модель процесса обнаружения сетевых аномалий (СА) в сети имеет следующие особенности.

1. Разнородный сетевой трафик представляется как совокупность дискретных сообщений $S_{k,1}^{n_{Uk,1}}$, где $n_{Uk,1}$ – номер сообщения от последнего по порядку источника сообщений U_k к первому по порядку источнику сообщений U_1; k - количество узлов в информационной системе (ИС).

2. После приема сообщения с номером $n_{Uk-1,1}$ могут иметь место следующие события:

– с вероятностью p прием сообщения с номером $n_{Uk,1}$;

– с вероятностью q потеря сообщения с номером $n_{Uk,1}$.

Вероятность приёма следующего сообщения после приёма/передачи предыдущего сообщения, обозначим как $P_{k,1}^{n_{Uk,1}}$ – переходная вероятность приёма сообщения $S_{k,1}^{n_{U_{k,1}}}$ с порядковым номером $n_{Uk,1}$ после приёма сообщения $S_{k,1}^{n-1_{U_{k,1}}}$, отправленного от k-го узла к первому.

В соответствии с принятой моделью предельные (установившиеся или равновесные) вероятности состояний P_{sk} определяются из условия нормировки

$$\sum_{j=1}^{n_{Um,n}} P_{m,n}^{j} = 1, \; m = \overline{1,k}, \; n = \overline{1,k}, \tag{8}$$

согласно которому

$$P_{sk} = \frac{1 - p/q}{1 - \left(p/q\right)^{n-k+1}} \left(\frac{p}{q}\right)^{j-k} \qquad j = k,\ldots,n. \tag{9}$$

Вероятности p и q связаны с заданным качеством сервиса в сети.

Таким образом, процесс является марковским только в моменты перехода. Однако в большинстве практически интересных задач можно игнорировать случайный характер времени ожидания и интересоваться только моментами перехода, поскольку сами значения состояний дают исчерпывающую информацию о функционировании системы

Как отмечалось выше, при выявлении аномального поведения и распознавании конкретных аномалий необходимо анализировать матрицы сигнатур или протоколов (детерминированный анализ) и статистических параметров. Результаты детерминированного анализа дают априорную информацию о состоянии сети. В дальнейшем буде рассматривать задачу анализа сигнатур, поскольку задача анализа протоколов не имеет никаких формальных отличий.

Запишем вектор сигнатур, для которых ранее были зарегистрированы аномалии, в следующем виде:

$$\mathbf{A}^T = \left\{a_1, a_2, ..., a_K\right\}, \tag{10}$$

где K – общее число аномалий; T – символ транспонирования.

Сигнатурой a_1 могут описываться следующие параметры: *поле* «адрес отправителя»; *поле* «адрес получателя»; *поле* «тип»; *поле* «данные»; *поле* «*CRC*».

В состав сигнатуры a_2 могут входить: *данны*е пакетов; *размер* пакетов; *время* получения пакетов; *время* отправления пакетов.

По сигнатуре a_3 определяются временные характеристики: *общая* продолжительность сеанса связи в сети; *время* установки соединения; *время* получения квитанций доставки и т.д.

Параметры сигнатур a_i входных данных сравниваются с параметрами сигнатур $\tilde{a}_j$ ожидаемых данных без аномалий. По результатам сравнения принимаются решения о наличии или отсутствии аномалии. Строится матрица решений вида

$$\mathbf{H}_A = \left\| h_{Aij} \right\| \text{ с элементами } \quad h_{A\,ij} = \begin{cases} 1, & a_i \notin \tilde{a}_j; \\ 0, & a_i \in \tilde{a}_j, \end{cases} \quad i, j \in \overline{1, K} \,. \tag{11}$$

Соответствующие значения элементов матрицы принимаются равными единице в случае выявления аномалии или нулю, если аномалии не выявлено. При этом значение $h_{A\,ij} = 0$ не может служить окончательным решением об отсутствии аномалии. Возможно, сигнатура (протокол) намеренно видоизменена или замаскирована.

Матрица решений (11) дает априорную информацию, которая в дальнейшем используется для построения информационной матрицы и получения границ ошибок оценок.

Совокупность *N* статистических показателей сетевого трафика обозначим

$$\mathbf{V}^T = \left\{ v_1, v_2, ..., v_N \right\}. \tag{12}$$

К таким показателям относятся вероятности ошибок первого и второго рода и моменты распределения, в частности, математические ожидания и дисперсии: *числа входящих IP*-пакетов в единицу времени; *числа исходящих IP*-пакетов в единицу времени; *числа входящих TCP*-пакетов в единицу времени; *числа исходящих TCP*-пакетов в единицу времени; *числа входящих UDP*-пакетов в единицу времени; *числа исходящих UDP*-пакетов в единицу времени; *размера* входящих пакетов; *времени* получения пакетов; *времени* отправления пакетов; *продолжительностей* сеансов связи в сети.

Оптимальной процедурой обнаружения аномалий с учетом предварительного детерминированного анализ сигнатур (протоколов) в самом общем случае является вычисление некоторого функционала эффективности

$$\Psi\left(\mathbf{H}_A, \mathbf{H}_V\right) \underset{A,V}{\rightarrow} \max, \tag{13}$$

где $\mathbf{H}_V = \mathbf{V}\mathbf{V}^T$. Матрицы $\mathbf{H}_A$ и $\mathbf{H}_V$ имеют размерность $K \times K$ и $N \times N$ соответственно, поэтому для конкретизации функционала (13) необходимо выбрать обобщенные параметры матриц и некую универсальную меру объединения множеств этих параметров. Данная задача рассматривается в следующем разделе.

Информация о состоянии сети периодически снимается с датчиков системы обнаружения аномалий. Если превышен пороговый уровень β_{0I}, принимается решение об обнаружении аномального поведения.

Следующими этапами являются распознавание типа аномалии, построение прогноза развития аномального состояния, оценка степени угрозы, выбор адекватных мер локализации и защиты. Эти вопросы в работе не рассматриваются.

Метод оценки параметров аномалий в условиях априорной неопределенности. При полной априорной информации о параметрах и состоянии системы байесовские асимптотически эффективные оценки вычисляются по критерию минимума среднего риска [11]. Однако ситуация наличия полной априорной информации является практически нереализуемой. Исходя из физического смысла решаемой задачи, ее следует отнести к классу задач с параметрической априорной неопределенностью [12]. Априорная неопределенность имеет место для некоторых параметров или для всей совокупности

параметров. Поэтому необходимо использовать другие оценки: минимаксные, максимума апостериорной плотности вероятности, максимального правдоподобия.

Общая оценка аномалии определяется по множеству параметров оценки, которые формируются так, как было описано в предыдущем разделе. Модель общей задачи оценки в рассматриваемой задаче содержит следующие компоненты.

1. Пространство параметров – выходных величин источников сообщений. Компоненты случайного вектора выходных величин $\mathbf{V}$ распределены по всей числовой оси, имеют математические ожидания m_{vi} и дисперсии σ_{vi}^2, $i=\overline{1,N}$.

2. Вероятностное отображение из пространства параметров в пространство наблюдений. По существу, это вероятностный закон, которым описывается влияние параметров вектора $\mathbf{V}$ на результаты наблюдений.

3. Пространство наблюдений (с конечным числом N измерений). Совокупность точек в этом пространстве представляет собой вектор размерностью N, который обозначим $\mathbf{R}$.

4. Правило оценки как статистическая процедура отображения точек v_i пространства наблюдений в точки $\hat{v}_i(\mathbf{R})$ пространства оценок. Каждой паре $\left[v_i, \hat{v}_i(\mathbf{R})\right]$ приписываются соответствующие потери, величина которых зависит от ошибки оценки $v_{i\varepsilon}(\mathbf{R}) = \hat{v}_i(\mathbf{R}) - v_i$.

На практике выбор конкретной функции потерь является результатом компромисса между требованиями удобства использования и принципиальной разрешимости задачи. Во многих представляющих интерес задачах одна и та же оценка может быть оптимальной (или хотя бы асимптотически оптимальной) для различных функций потерь. Специфической особенностью рассматриваемой задачи является разное отношение наблюдателя к знаку ошибки. В такой ситуации функция потерь должна быть асимметричной. Кроме того, в данной задаче наибольший интерес представляют результаты анализа потерь, искажений, модификации информации, т.е. получение неких оценок по информационным критериям. Соответственно, целесообразно применять информационные функции потерь.

В качестве информационной функции потерь обычно выбирают функцию наиболее общего вида [12]:

$$C\left(\hat{v}_i, v_i\right) = -\ln W\left(v_i \mid \hat{v}_i\right), \tag{14}$$

где $W\left(v_i \mid \hat{v}_i\right)$ – условная плотность вероятности (ПВ) параметра v_i, если принята оценка $\hat{v}_i$.

Заметим, что в условиях высокой апостериорной точности и, соответственно, нахождения оценки $\hat{v}_i$ в малой ε-окрестности точки v_i можно применять метод гауссовой аппроксимации условной ПВ. В этом случае функция (14) будет симметричной, что упрощает задачу оптимального оценивания.

Для минимизации функции потерь необходимо усреднить ее по всем возможным значениям выборки наблюдаемых данных и найти минимум функции:

$$\mathcal{R}\left(\hat{v}_i\right) = \int C\left(\hat{v}_i, v_i\right) W\left(v_i\right) dv_i \underset{\hat{v}_i}{\rightarrow} \min,$$

или, с учетом (14)

$$\mathcal{R}\left(\hat{v}_i\right) = -\int \ln W\left(v_i \mid \hat{v}_i\right) W\left(v_i\right) dv_i \underset{\hat{v}_i}{\rightarrow} \min, \tag{15}$$

который можно трактовать как апостериорный риск при анализе выборки наблюдаемых данных фиксированного объема.

Математическое ожидание параметра v_i обозначим $m_{vi} = E\left[v_i\right]$, а дисперсию $\sigma_{vi}^2 = E\left[\left(v_i - m_{vi}\right)^2\right]$.

Минимум апостериорного риска (15) при гауссовой аппроксимации условной ПВ достигается путем минимизации ошибки оценки $\hat{v}_i(\mathbf{R})$. В качестве усредненной оценки

количества априорной информации, полученной по результатам детерминированного анализа матрицы (11), используем Евклидову норму [13]:

$$\|\mathbf{H}\| = \left(\sum_{i,j} \left| h_{Aij} \right| \right)^{1/2} = H_R .$$

Представим математическое ожидание оценки в виде взвешенной суммы $c_1 m_{vi} + c_2 H_R = B_{Ri}$. Весовые коэффициенты c_1 и c_2 выбираются из условия нормировки: $c_1 + c_2 = 1$. Тогда дисперсия оценки $\sigma^2_{Hvi} = E\left[\left(\hat{v}_i(R) - B_{Ri} \right)^2 \right]$.

Таким образом, получаем несмещенную оценку B_{Ri}, которая удовлетворяет неравенству Крамера – Рао [12]:

$$\sigma^2 \left[\hat{v}_i(\mathbf{R}) - B_{Ri} \right] \geq \left(E\left\{ \left[\frac{\partial \ln p_{r|vi}(\mathbf{R} \mid B_{Ri})}{\partial B_{Ri}} \right]^2 \right\} \right)^{-1}, \qquad (16)$$

где предполагается, что производные в правой части существуют и абсолютно интегрируемы. Если оценка удовлетворяет указанной границе со знаком равенства, она является эффективной и представляет собой единственное решение уравнения правдоподобия $\frac{\partial \ln p_{r|vi}(\mathbf{R} \mid B_{Ri})}{\partial B_{Ri}} = 0$ при $B_{Ri} = \hat{v}_{ml}(\mathbf{R})$, где $\hat{v}_{ml}(\mathbf{R})$ – максимально правдоподобная оценка.

Асимптотические свойства оценок исследуются в процессе изменения ошибки при неограниченном увеличении числа независимых наблюдений или при неограниченном уменьшении количества мешающей информации.

Поскольку оценка является несмещенной и эффективной, ее дисперсия σ^2_{Hvi} удовлетворяет неравенству

$$\sigma^2_{Hvi} = \sigma^2 \left[\hat{v}_i(R) - B_{Ri} \right] \geq J^{ii}, \qquad (17)$$

где J^{ii} является диагональным элементом квадратной матрицы $\mathbf{J}^{-1}$ размерностью $N \times N$ – так называемой информационной матрицы Фишера [12]. Элементы матрицы определяются, в соответствии с (16), следующим образом:

$$J_{ij} = E\left[\frac{\partial \ln p_{r|v}(\mathbf{R} \mid \mathbf{V})}{\partial v_i} \frac{\partial \ln p_{r|v}(\mathbf{R} \mid \mathbf{V})}{\partial v_j} \right] = -E\left[\frac{\partial^2 \ln p_{r|v}(\mathbf{R} \mid \mathbf{V})}{\partial v_i \partial v_j} \right]. \qquad (18)$$

Поскольку в рассматриваемой задаче имеются как детерминированные, так и случайные параметры, матрица Фишера состоит из двух слагаемых:

$$\mathbf{J} = \mathbf{J}_V + \mathbf{J}_H , \qquad (19)$$

где $\mathbf{J}_H$ содержит информацию, полученную в результате детерминированного анализа сигнатур и используемую в дальнейшем в качестве априорной информации, а $\mathbf{J}_V$ дает информацию, полученную по результатам статистического анализа.

Матрица $\mathbf{J}_H$ является диагональной с элементами $J_{Hii} = \sigma^2_{Hvi} = E\left[\left(\hat{v}_i(R) - B_{Ri} \right)^2 \right]$. Следовательно, диагональные элементы в матрице, которая является обратной к полной информационной матрице (19), есть нижние границы соответствующих средних квадратов ошибок.

В заключение выведем выражение для асимптотической ошибки апостериорной оценки при использовании информационной функции потерь (14) и гауссовой аппроксимации

условной ПВ. При стремлении весового коэффициента c_1 к единице (соответственно, при $c_2 \to 0$)

$$J_{ii} = E\left[\frac{\partial \ln p_v(\mathbf{V})}{\partial v_i}\right]^2 = \left[\frac{(v_i - m_{vi})}{\sigma_{vi}^2}\right]^2, \qquad (20)$$

т.е. получаем квадратичную зависимость потерь от ошибок оценки.

Таким образом, используя полученные выражения (17)…(20), можно получить асимптотические оценки статистических характеристик ошибок при использовании разработанного комбинированного метода обнаружения аномалий в поведении сетевых и терминальных узлов корпоративной сети.

Литература

1. Виноградов Н. А. Анализ потенциальных характеристик устройств коммутации и управления сетями новых поколений / Н. А. Виноградов // Зв'язок. – 2004. – №4. – С. 10-17.

2. Анализ нагрузки на сети передачи данных в системах критичного применения / Н. А. Виноградов, В. И. Дрововозов, Н. Н. Лесная, А. С. Зембицкая // Зв'язок. – 2006. – №1. – С. 9-12.

3. Корниенко А.А. Системы и методы обнаружения вторжений: современное состояние и направления совершенствования [Електронний ресурс] / А. А. Корниенко, И. М. Слюсаренко // Режим доступу : www.citforum.ru

4. Бауэр Ш. Что же сегодня норма? [Електронний ресурс] / Ш. Бауэр, А. Хельвиг // LAN – Журнал сетевых решений // Режим доступу : http://www.osp.ru/lan/2006/06/2414964/

5. Аграновский А. В. Новый подход к защите информации – системы обнаружения компьютерных угроз [Електронний ресурс] / А. В. Аграновский, Р. А. Хади // Jet Info №4 // Режим доступу : http://www.jetinfo.ru/2007_detail

6. Шеридан Т. Б. Системы человек – машина: Модели обработки информации, управления и принятия решений человеком-оператором / Шеридан Т. Б., Феррел У. Р. ; пер. с англ. под ред. К. В. Фролова. – М.: Машиностроение, 1980. – 400 с.

7. Попов Г. П. Инженерная психология в радиолокации (система человек-оператор) / Г. П. Попов. – М.: Сов. радио, 1971. – 144 с.

8. Тихонов В. И. Марковские процессы / В. И. Тихонов, М. А. Миронов. – М.: Сов. радио, 1977. – 488 с.

9. Вопросы статистической теории распознавания / [Ю. Л. Барабаш, Б. В. Варский, В. Т. Зиновьев и др.] – М.: Сов. радио, 1967. – 400 с.

10. Вальд А. Последовательный анализ / А. Вальд. – М.: Физматгиз, 1960. – 606 с.

11. Леман Э. Проверка статистических гипотез / Э. Леман. – М.: Наука, 1979. – 408 с.

12. Репин В.Г. Статистический синтез при априорной неопределенности и адаптация информационных систем / В. Г. Репин, Г. П. Тартаковский. – М.: Сов. радио, 1977. – 432 с.

13. Фаддеев Д. К. Вычислительные методы линейной алгебры / Д. К. Фадеев, В. Н. Фадеева. – М.: Физматгиз, 1963. – 656 с.