УДК 519.876.5:004.056.53

В.С. Ловягин, аспирант
Севастопольский национальный технический университет
ул. Университетская 33, г. Севастополь, Украина, 99053
E-mail: lovyagin88@gmail.com

СТАТИСТИЧЕСКИЙ МОНИТОРИНГ ВИРУСНЫХ АТАК НА ОСНОВЕ ПАРАМЕТРИЧЕСКИХ КРИТЕРИЕВ

В статье исследуется эффективность и применимость статистических методов мониторинга вирусных атак, происходящих в компьютерных системах, основанных на параметрических критериях. Для получения статистических данных был использован разработанный авторами имитационный стенд.

Ключевые слова: *мониторинг, статистические методы мониторинга, вирусная атака, параметрические критерии.*

В настоящее время возникла необходимость исследования эффективности и применимости различных методов мониторинга состояния компьютерных систем (КС), в том числе мониторинг наличия вирусных атак (ВА) в системе. В работах [1, 2, 4] рассматриваются и описываются статистические параметрические критерии, описывается способ их применения к случайным выборкам, однако проблема применимости данных критериев в отношении безопасности КС не рассматривалась до настоящего времени. Мониторинг является составной частью процесса обеспечения безопасности КС. Кроме мониторинга обеспечение безопасности включает принятие решения о качественном и количественном составе мер противодействия КС, принятие мер по устранению потерь от успешных ВА. Основными задачами процесса мониторинга и диагностики является выявление наличия вирусных атак и определение интенсивности атак. На основе данных, получаемых от мониторинга и диагностики состояния КС, система поддержки принятия решения (СППР) должна обеспечивать возможность выбора количественного и качественного состава мер противодействия ВА. Данное решение должен принимать эксперт — администратор системы.

Целью данной статьи является исследование эффективности и применимости статистических методов мониторинга вирусных атак на основе параметрических критериев. Объектом исследования являются статистические методы мониторинга вирусных атак, основанные на параметрических критериях. Предметом исследования является имитационный стенд, основанный на имитационной модели узла КС.

Рассмотрим типичный узел КС (рисунок 1) на который может производиться вирусная атака (ВА), где L — буферный элемент, хранящий очередь запросов к узлу КС, время обслуживания объектом КС запроса — T_{obs}. Запросы от субъектов КС поступают в буферный элемент L, затем непосредственной в узел КС, вирусные атаки также поступают в буферный элемент. Для обеспечения поддержки принятия решения о применении контрмер администратором системы (ЛПР) служит система поддержки принятия

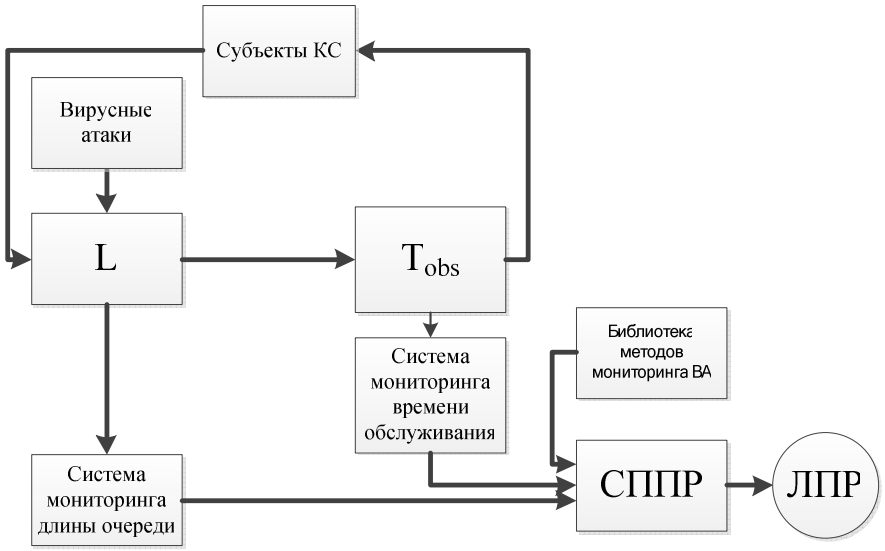

Рисунок 1 — Типичная структура узла КС

решения (СППР), получающая информацию от систем мониторинга длины очереди буферного элемента, времени обслуживания запросов от субъектов КС. СППР генерирует советы для ЛПР базируясь на библиотеке методов мониторинга ВА.

В данной работе под понятием вирусная атака следует понимать попытки субъектов КС получить несанкционированный доступ к узлам КС.

Входной поток заявок, поступающий в буферный элемент, примем простейшим однородным.

Процесс выявления вирусной атаки в узле КС многоэтапный и включает в себя:

— определение наличия ВА на основе сбора статистических данных о динамики изменения длины очереди l запросов в буферном элементе;

— принятие решения о наличии ВА на основе статистических данных;

— классификацию ВА на основе «знаний» полученных системой диагностики вирусных атак (СДВА) в результате самообучения и данных, полученных от предыдущих двух этапов.

На этапе сбора статистических данных о длине очереди для обнаружения вирусной атаки следует производить мониторинг длины очереди буферного элемента с интервалом времени τ_1. Очевидно, что интервал времени τ_1 должен обеспечивать возможность нахождения вирусной атаки в узле, но при этом, не занимать узел на время превышающее предельно допустимое h_1.

В процессе данной проверки узла все связи буферного элемента блокируются на интервал времени $\Delta\tau_1$, необходимый для подсчета длины очереди.

Возможен аналогичный сбор статистических данных о времени обработки запросов от субъектов КС к объектам КС. В процессе функционирования узла КС необходимо производить временные замеры (t_1, t_2) для запросов на входе и на выходе обрабатывающего устройства. Через промежутки времени τ_2 по полученным в ходе сбора статистики данным строится гистограмма распределения времени пребывания запросов в очереди.

Определение отсутствия атаки производится путем проверки статистической гипотезы H_0 о принадлежности двух выборок одной генеральной совокупности. Принятие конкурирующей с ней гипотезы H_1 должно подтверждать наличие атаки в КС.

В данной работе рассмотрим три основные способа проверки статистической гипотезы описанные в [1, 2]:

— нахождение значения критерия Фишера;

— нахождение значения критерия Кокрена;

— нахождение значения критерия Стьюдента.

Однако следует отметить, что данные критерии применимы исключительно для выборок распределенных по нормальному закону распределения. С целью проверки нормальности выборок следует проверять выборку по одному из критериев нормальности предложенных в [3]. В данной работе будет применяться критерий Шапиро-Уилка, для удобства вычислений применяться будет вариант критерия, аппроксимированный для $\alpha = 0{,}05$ [4].

Для решения задачи исследования эффективности статистических методов мониторинга основанных на параметрических критериях предлагается использование имитационного стенда. Ниже перечислим основные функции имитационного стенда:

— моделирование поведения узла КС с различными параметрами;

— моделирование ВА в узле различных интенсивностей;

— сбор и обработка статистических данных согласно методу, выбранному из библиотеки методов диагностики;

— принятие решения о наличии ВА в КС.

Согласно перечисленным функциям предлагается структура имитационного стенда, предоставленная на рисунке 2.

Узел КС, структура которого была предоставлена на рисунке 1, возможно описать в терминах теории массового обслуживания. Так субъекты КС могут представляться совокупностью генераторов заявок, узел КС — обслуживающим устройством, буферный элемент L — очередью. Имитационная модель узла КС разработана в программной среде *AnyLogick 5.4.1*.

С помощью данных, получаемых при работе имитационного стенда, были исследованы диапазоны значений интенсивностей атак, для которых статистические методы мониторинга и диагностики давали устойчивы безошибочные подтверждения наличия вирусных атак в КС. В таблице 1 приведены значения критериев Фишера, Кокрена, Стьдента для данных, полученных в ходе проведения трех экспериментов. На рисунке 3 приведены графики зависимостей средних значений критериев Фишера, Кокрена, Стьюдента от интенсивностей атак. В данных экспериментах интенсивность нормальных запросов $\lambda_{норм} = 2{,}2$ запросов в секунду (з/с), интенсивность обработки запросов в узле КС $\mu = 4{,}3$ (з/с). Критические значения для критериев приведены в таблице 2.

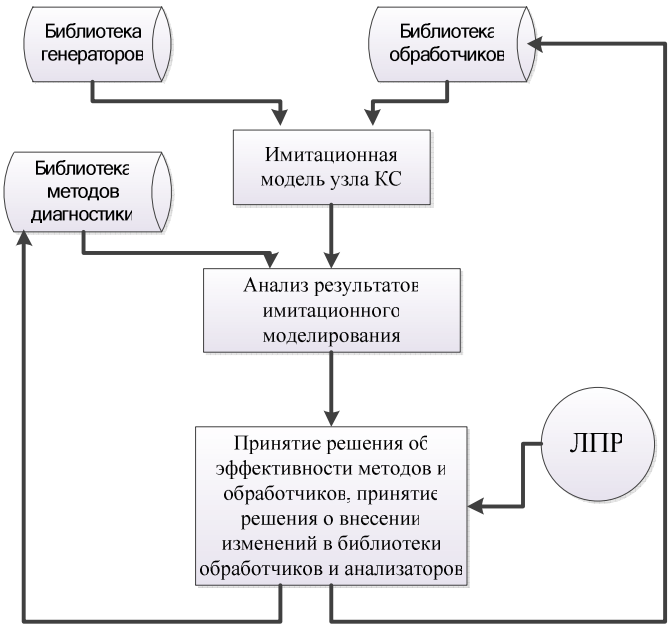

Рисунок 2 — Упрощенная структурная схема имитационного стенда для исследования эффективности методов мониторинга и диагностики атаки в КС

Таблица 1 — Значения критериев Фишера, Кокрена, Стьюдента для данных полученных в ходе проведения экспериментов, с использованием имитационного стенда (серым цветом выделены ячейки, в которых значения критерия превышают критические)

Интенсивность ВА (ед/с)	критерий Фишера				критерий Кокрена				критерий Стьюдента			
	эксперимент №1	эксперимент №2	эксперимент №3	среднее значение	эксперимент №1	эксперимент №2	эксперимент №3	среднее значение	эксперимент №1	эксперимент №2	эксперимент №3	среднее значение
8,292	41,863	48,150	45,336	45,116	1,000	1,000	1,000	1,000	8,996	9,648	9,362	9,336
2,800	46,023	63,142	50,107	53,091	1,000	1,000	1,000	1,000	9,433	11,049	9,005	9,829
1,681	15,047	56,829	27,596	33,157	0,986	0,973	0,968	0,976	5,394	10,482	3,596	6,491
1,194	5,549	29,256	14,648	16,484	0,962	0,999	0,990	0,984	3,275	7,521	5,317	5,371
0,944	7,716	7,864	8,662	8,081	0,915	0,792	0,690	0,799	3,862	3,899	4,072	3,944
0,767	7,572	4,676	12,823	8,357	0,775	0,780	0,994	0,850	3,826	3,007	4,664	3,832
0,650	5,254	7,181	8,016	6,817	0,630	0,999	0,843	0,824	3,187	3,726	3,930	3,614
0,564	4,070	7,158	4,091	5,106	0,771	0,995	0,993	0,919	2,805	3,720	2,812	3,112
0,497	3,655	3,232	3,525	3,471	0,718	0,997	0,988	0,901	2,658	2,500	2,608	2,589
0,444	2,197	4,163	3,178	3,179	0,861	0,966	0,933	0,920	2,061	2,837	2,467	2,455
0,400	2,243	4,632	2,682	3,186	0,736	0,992	0,974	0,900	2,082	2,993	2,265	2,447
0,367	4,577	0,835	1,549	2,320	0,807	0,942	0,947	0,899	2,975	1,271	1,724	1,990
0,342	4,291	1,789	2,290	2,790	0,558	0,946	0,977	0,827	2,880	1,860	2,076	2,272
0,317	2,070	1,456	1,310	1,612	0,732	1,000	0,964	0,899	2,001	1,678	1,589	1,756
0,292	0,122	3,389	5,339	2,950	0,552	0,955	0,889	0,799	0,485	2,560	3,210	2,085
0,275	4,367	0,202	3,267	2,612	0,712	0,989	0,972	0,891	2,906	0,624	2,335	1,955
0,258	0,880	2,950	1,468	1,766	0,616	1,000	0,890	0,835	1,304	2,388	1,658	1,783
0,242	0,054	2,580	0,985	1,206	0,519	0,940	0,921	0,793	0,324	2,233	1,378	1,312
0,233	1,502	1,690	1,599	1,597	0,523	0,979	0,977	0,827	1,704	1,808	1,749	1,754
0,219	0,079	1,359	1,760	1,066	0,609	0,801	1,000	0,803	0,392	1,621	1,800	1,271
0,208	0,587	0,848	1,749	1,061	0,582	0,982	0,980	0,848	1,065	1,280	1,817	1,388
0,200	0,001	1,088	0,280	0,456	0,566	1,000	0,994	0,853	0,038	1,450	0,721	0,737
0,192	1,876	0,632	0,112	0,873	0,657	0,998	0,961	0,872	1,904	1,105	0,460	1,157

Таблица 2 — Критические значения критериев Фишера, Кокрена, Стьюдента для $\alpha = 0{,}05$

критерий Фишера	1,84
критерий Кокрена	0,777
критерий Стьюдента	3,646

Рисунок 3 — График зависимости параметрических критериев, от интенсивности входного потока атак на узел КС для трех экспериментов: а) критерий Фишера; б) критерий Кокрена; в) критерий Стьюдента

Из приведенных выше графиков следует сделать вывод о применимости каждого из рассмотренных методов с целью диагностики состояния безопасности КС. Очевидно, что диагностика

состояния безопасности с использованием вычисления критерия Фишера дает устойчивый результат при интенсивности атак выше 0,4 (з/с), для критерия Кокрена устойчивый результат достигается при интенсивности атак выше 1,7 (з/с), для критерия Стьюдента устойчивый результат при интенсивности атак выше 1,2 (з/с).

Из полученных результатов исследования следует, что статистические методы недостаточно эффективны при малых интенсивностях ВА, что уменьшает область применения данных методов.

Следует отметить недостатки рассмотренных статистических методов мониторинга и диагностики:

— необходимость сбора большой статистики для применения методов, что требует временных затрат;

— невозможность обнаружения единичных вирусных атак или атак с низкой интенсивностью.

Несмотря на перечисленные недостатки, существует ряд преимуществ данных методов:

— высокое быстродействие;

— малые затраты процессорного времени на вычисление параметрических критериев;

— низкие затраты на обслуживание.

Данные методы диагностики возможно применять в случаях некритичности появления единичных атак в системе и первоочередной задачи поддержания системы в стационарном режиме (режиме без переполнения очереди). В иных ситуациях данные методы не применимы.

В качестве дальнейшего развития проблемы предполагается исследование эффективности методов мониторинга, основанных на непараметрических критериях.

Библиографический список использованной литературы

1. Митропольский А.К. Техника статистических вычислений / А.К. Митропольский. — М.: Физматгиз, 1961. — 480 с.

2. Большев Л.Н. Таблицы математической статистики / Л.Н. Большев, Н.В. Смирнов; под ред. Большева Л.Н. — М.: Наука, 1983. — 416 с.

3. Кобзарь А.И. Прикладная математическая статистика / А.И. Кобзарь. — М.: Физматлит, 2006. — 816 с.

4. Shapiro S.S. An analysis of variance test for normality / S.S. Shapiro, M.B. Wilk // Biometrika. — 1965. — № 3. — P. 591–611.

Поступила в редакцию 21.01.2011 г.

Ловягін В.С. Статистичний моніторинг вірусних атак на основі параметричних критеріїв

У статті досліджується ефективність і застосовність статистичних методів моніторингу вірусних атак, що відбуваються в комп'ютерних системах, які засновані на параметричних критеріях. Для отримання статистичних даних був використаний імітаційний стенд, який розробили автори.

Ключові слова: моніторинг, статистичні методи моніторингу, вірусна атака, параметричні критерії.

Lovyagin V.S. Statistical monitoring of virus attacks based on parametric criteria

The effectiveness and applicability of statistical methods for monitoring virus attacks based on parametric criteria are investigated. The simulation stand developed by the authors is used for obtaining statistical data.

Keywords: monitoring, statistical monitoring method, virus attack, parametric criteria.