

УДК 621.3

А.А. Кузнецов<sup>1</sup>, А.В. Северинов<sup>1</sup>, С.Н. Симоненко<sup>1</sup>, О.И. Качур<sup>2</sup><sup>1</sup>Харьковский университет Воздушных Сил им. И. Кожедуба, Харьков<sup>2</sup>Харьковский национальный университет радиоэлектроники, Харьков

## МЕТОД ДЕТЕКТИРОВАНИЯ ВИРУСНЫХ АТАК НА ОСНОВЕ АНАЛИЗА СЕТЕВОГО ТРАФИКА

Рассматриваются вопросы детектирования вирусных атак на основе анализа сетевого трафика мультисервисных сетей с помощью BDS-теста. Предложен новый подход к детектированию сетевых вирусных атак. Приводятся результаты экспериментальных исследований различных видов сетевого трафика BDS-тестом, позволяющие определить наличие вирусного воздействия.

**Ключевые слова:** BDS-тест, вирусная атака, вредоносное программное обеспечение, обнаружение вирусных атак.

### Введение

Широкое применение компьютерной техники в современных системах вооружения и военной техники, таких как автоматизированная система управления "Ореанда", привело к появлению таких видов угроз безопасности данных систем, как воздействие программ-вирусов, способных не только нанести огромный ущерб информации, которая хранится и обрабатывается на компьютерах системы, но и полностью вывести из строя систему управления.

В связи с этим на сегодняшний день проблема борьбы с компьютерными вирусами чрезвычайно актуальна. Вирусные атаки получили широкое распространение. На противодействие вирусам выделяется большое количество ресурсов. Однако количество известных вирусных атак неуклонно растет и не существует методов, которые бы позволили решить данную проблему окончательно.

**Цель данной статьи** – предложить новый подход к детектированию сетевых вирусных атак. Этот подход основан на применении BDS-статистики для анализа сетевого трафика. Данный метод является развитием метода идентификации сетевого трафика [1], который широко используется для оптимизации использования ресурсов сети.

В основе метода детектирования сетевых вирусных атак лежит представление сетевого трафика в виде временных рядов, которые обрабатываются известным BDS-тестом. Этот тест был разработан W.A. Brock, W. Dechert J. Scheinkman в 1987 году для анализа временных рядов финансовых рынков [2] и позволяет выявлять зависимости во временных данных и проверить гипотезу о том, что значения временного ряда независимы и одинаково распределены.

Известны работы по применению BDS-теста для идентификации сетевого трафика [1], а также для обнаружения хаотических сигналов на фоне белого шума [3].

### Результаты исследований

BDS-тест основан на расчете статистической величины  $w(\tilde{\xi})$  (BDS-статистике)

$$w_{m,N}(\varepsilon) = \sqrt{N-m+1} \frac{C_{m,N}(\varepsilon) - (C_{1,N-m}(\varepsilon))^m}{\sigma_{m,N}(\varepsilon)}, \quad (1)$$

где  $m$  - размерность пространства вложения;  $N$  - число элементов временного ряда;  $\varepsilon$  - радиус гиперсферы;  $\sigma_{m,N}(\varepsilon)$  - среднеквадратическое отклонение;  $C_{m,N}(\varepsilon)$ ,  $C_{1,N}(\varepsilon)$  - корреляционные интегралы.

В основе расчета значения BDS-теста лежит вычисление разности корреляционных интегралов. W. Brock, W. Dechert, J. Scheinkman показали, что

$$C_{m,N}(\varepsilon) \Rightarrow C_{1,N}(\varepsilon)^m$$

со стопроцентной вероятностью при  $N \rightarrow \infty$ , а

$$\left( C_{m,N}(\varepsilon) - (C_{1,N}(\varepsilon))^m \right) \cdot \sqrt{N-m+1}$$

является случайной асимптотически нормально распределенной величиной с нулевым средним и среднеквадратическим отклонением  $\sigma_{m,N}(\varepsilon)$ .

В отсутствие шумов наблюдения применение критерия значимости к статистике  $w_{m,N}(\varepsilon)$  позволяет эффективно решать задачу классификации наблюдения. В работе [4] предложены быстрые методы расчета BDS-теста.

Предлагается использование BDS-теста для выявления вредоносного воздействия компьютерных вирусов. На рис. 1 представлены этапы методики проведения экспериментальных исследований свойств различных типов сетевого трафика.

Предложенная методика предусматривает захват информационного трафика и его формализацию в виде временных рядов. На основе результатов BDS-тестирования временных рядов делается вывод о наличии вредоносного воздействия.

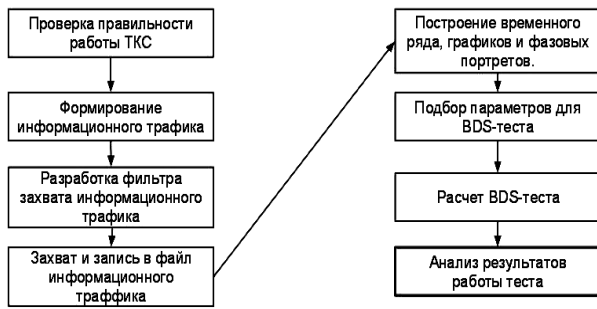


Рис. 1. Методика проведения экспериментальных исследований

На рис. 2 представлена структурная схема модуля анализа трафика и принятия решений

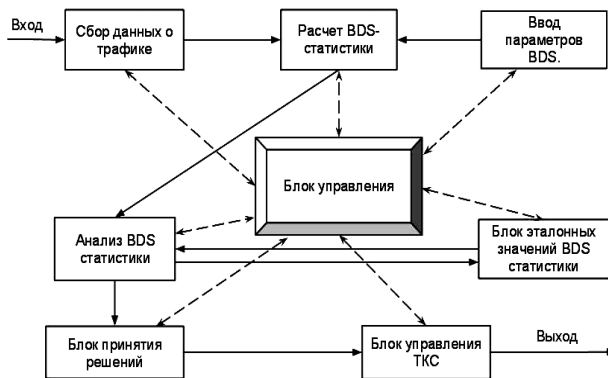


Рис. 2. Структурная схема модуля анализа трафика и принятия решений

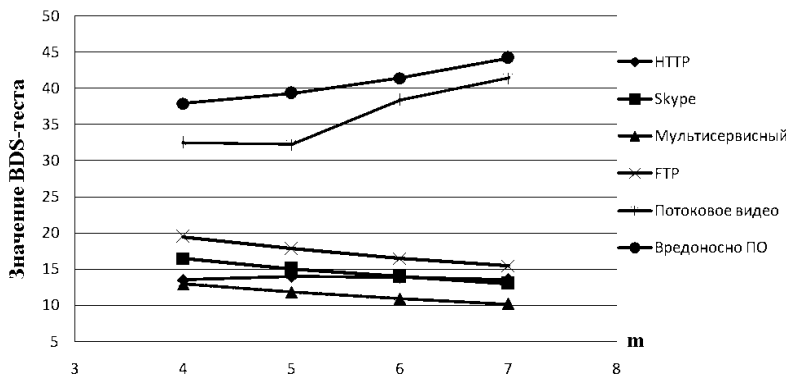


Рис. 3. Зависимость значений BDS теста от параметра  $\epsilon=0.5\sigma$

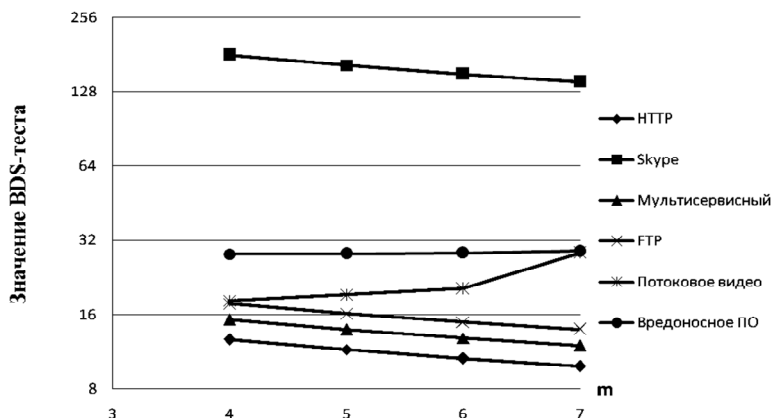


Рис. 4. Зависимость значений BDS теста от параметра  $m, \epsilon=\sigma$

На вход модуля анализа трафика подается исследуемый трафик, который подвергается дальнейшей обработке и анализу с помощью BDS-статистики. На основе сравнения рассчитанных значений с эталонными блок принятия решений формирует результат в виде сообщения о нормальной работе системы или о выявленной вирусной атаке. Решение о вирусной атаке принимается в случае, когда эталонные значения для вирусных атак сходятся с экспериментально полученными, либо полученная статистика не соответствует ожидаемой для данного режима работы автоматизированной системы, что может служить сигналом о воздействии вредоносного программного обеспечения (ПО).

Результаты BDS теста принимают различные значения в зависимости от выбранных параметров.

На рис. 3, 4 представлены результаты значений BDS теста при различных параметрах  $\epsilon, m$ .

В результате проведенных исследований были сформированы практические рекомендации по построению средств защиты компьютерных сетей от вирусных атак.

Проведенные расчеты подтверждают теоретические предположения о том, что для различных видов трафика результат BDS-теста дает различные значения, которые могут быть приняты в качестве эталонных.

В табл. 1 представлены усредненные значения BDS-тестов для различных видов трафика, полученные в результате проведенных экспериментальных исследований.

В компьютерной сети автоматизированной системы сетевые службы могут использоваться одновременно, что приведет к изменению значений BDS-теста. Однако наличие в сетевом трафике следов вредоносного ПО приведет к соответствующему изменению значений BDS-статистики.

На рис. 5 представлены усредненные значения BDS-тестов для различных видов трафика при  $\epsilon=0.5\sigma$ .

Таким образом экспериментальные данные подтвердили теоретическое предположение о возможности использования значений BDS-теста для детектирования следов вредоносного ПО в сетевом трафике.

Предложенный метод детектирования вирусных атак может быть использован в антивирусных системах, а также в качестве дополнительного компонента системы обнаруже-

ния вторжений в качестве сенсорной (датчики по сбору информации о трафике) и аналитической части (компонент модуля принятия решений) (рис. 6).

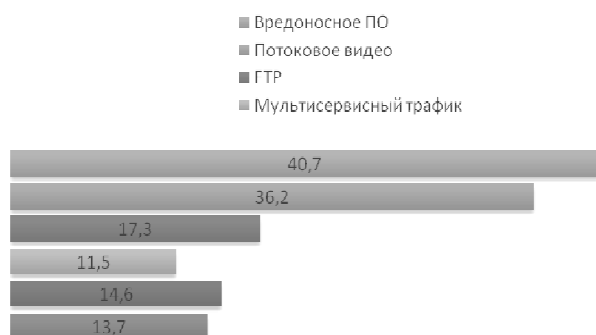


Рис. 5. Сравнение усредненных характеристик BDS-теста для различных служб

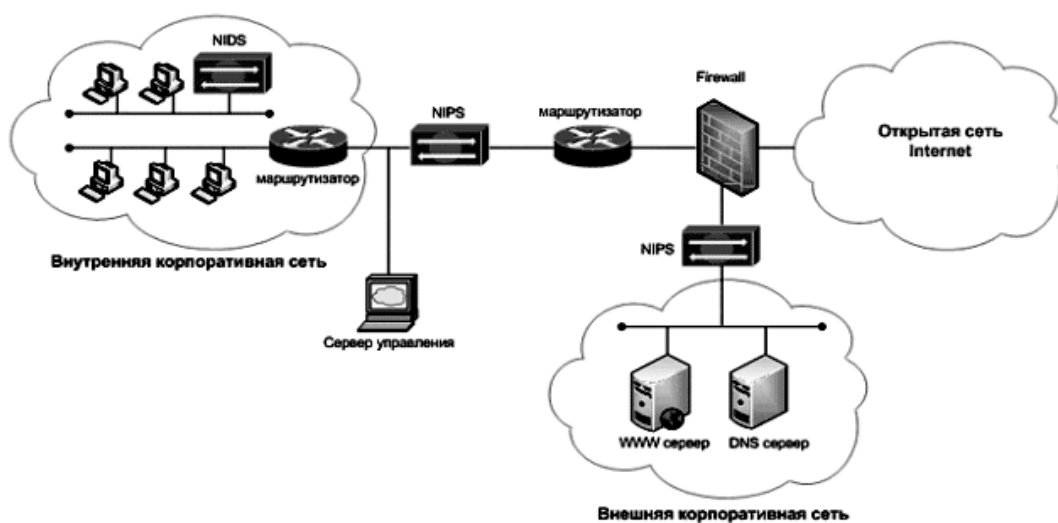


Рис. 6. Типичная схема подключения IDS, IPS системы

## Выводы

Таким образом, разработанный метод детектирования вирусных атак на основе анализа сетевого трафика может быть использован в системах защиты современных систем автоматизированного управления, как в качестве основного, так и дополнительного средства выявления вредоносного программного обеспечения.

Проведенные экспериментальные исследования, подтверждают теоретические предпосылки к использованию BDS-статистики в качестве основы для выявления вирусных атак, а также возможность построения на их основе систем обнаружения вредоносного программного обеспечения при вирусной атаке.

Направление дальнейших исследований – создание расширенной базы эталонов значений, полученных с помощью BDS-тестов, с целью применения для анализа различных сетевых служб современных автоматизированных систем управления вооружением и военной техникой.

Таблица 1  
Усредненные значения BDS-тестов для различных видов трафика

Усредненные значения BDS-тестов		
Вид сервиса	$\epsilon=0.5 \sigma$	$\epsilon=\sigma$
HTTP	13,7	11,2
Skype	14,6	171,9
Мультисервисный трафик	11,5	13,5
FTP	17,3	15,7
Потоковое видео	36,2	21,6
Вредоносное ПО	40,7	28,5

## Список литературы

1. Кузнецов А.А. Метод структурной идентификации потоков в телекоммуникационных сетях на основе BDS-тестирования / А.А. Кузнецов, С.Г. Семенов, С.Н. Симоненко, Е.В. Мелешко // Наука і техніка Повітряних Сил ЗС України. – 2010. - № 2(4). – С. 131-136.
2. Brock W. A test for independence based on the correlation dimension / W. Brock, W. Dechert, J. Scheinkman. – Working Paper, University of Wisconsin, 1987. – 120 p.
3. Костенко П.Ю. Непараметрический BDS – обнаружитель хаотических сигналов на фоне белого шума. // П.Ю. Костенко, А.Н. Барсуков, К.С. Васюта, С.Н. Симоненко // Збірник наукових праць ХВПС. – X.: ХВПС, 2010. – Вип. 3 (25). – С. 108-116.
4. LeBaron B. A Fast Algorithm for the BDS Statistic / B. LeBaron // Studies in Nonlinear Dynamics and Econometrics. – 1997. – Vol. 2, No. 2. – P. 53-59.
5. A test for independence based on correlation dimension / W. Brock, W. Dechert, J. Scheinkman, B. LeBaron // Econometric Reviews. – 1996. – 15. – P. 197-235.

Поступила в редакцию 1.03.2011

Рецензент: д-р тех. наук, проф. Ю.В. Стасев, Харьковский университет Воздушных Сил имени И. Кожедуба, Харьков.

**МЕТОД ДЕТЕКТУВАННЯ ВІРУСНИХ АТАК НА ОСНОВІ АНАЛІЗУ МЕРЕЖЕВОГО ТРАФІКУ**

О.О. Кузнецов, О.В. Северінов, С.М. Симоненко О.І. Качур

*Розглядаються питання детектування вірусних атак на основі аналізу мережевого трафіку мультисервісних мереж за допомогою BDS-тесту. Запропоновано новий підхід до детектування мережевих вірусних атак. Наводяться результати експериментальних досліджень різних видів мережевого трафіку BDS-тестом, що дозволяють визначити наявність вірусного впливу.*

**Ключові слова:** BDS-тест, вірусна атака, шкідливе програмне забезпечення, виявлення вірусних атак.

**METHOD OF DETECTION OF VIRAL ATTACKS ON BASIS OF ANALYSIS OF NETWORK TRAFFIC**

A. A. Kuznetsov, A. V. Severinov, S. N. Simonenko, O. I. Kachur

*The questions of detection of viral attacks are examined on the basis of analysis of network traffic of multiservice networks by a BDS-test. The new going is offered near detection of network viral attacks. Results over of experimental researches of different types of network traffic are brought by a BDS-test, allowing to define the presence of viral influence.*

**Keywords:** BDS-test, viral attack, malware software, finding out viral attacks.