Sergei G. Semenov[1], Svitlana Y. Gavrylenko[2], Victor V. Chelak[3]

DEVELOPING PARAMETRICAL CRITERION FOR REGISTERING ABNORMAL BEHAVIOR IN COMPUTER AND TELECOMMUNICATION SYSTEMS ON THE BASIS OF ECONOMIC TESTS

In this article a study of malicious attacks' detection methods of computer and telecommunication systems is conducted. The need to improve the IT models and to substantiate the choice of criteria for assessing the abnormal behavior in computer and telecommunication systems is revealed. The appropriateness of using the jitter of the BDS-test value as an indicator of abnormal behavior in computer and telecommunication systems, and the percentage of deviation in the presented value from the values chosen as a result of the experiment as the grading criteria is grounded.

Keywords: *computer and telecommunication systems; abnormal behavior; BDS-test.*

Сергій Г. Семенов, Світлана Ю. Гавриленко, Віктор В. Челак

РОЗРОБКА ПАРАМЕТРИЧНОГО КРИТЕРІЮ РЕЄСТРАЦІЇ АНОМАЛЬНОЇ ПОВЕДІНКИ КОМП'ЮТЕРНИХ ТА ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ НА ОСНОВІ ЕКОНОМІЧНИХ ТЕСТІВ

У статті досліджено методи виявлення злочинних атак на комп'ютерні та телекомунікаційні системи. Виявлено необхідність удосконалення моделей інформаційних технологій та аргументованого вибору критеріїв для оцінювання аномальної поведінки комп'ютерних і телекомунікаційних систем. Доведено доцільність використання у вигляді показника аномальної поведінки комп'ютерної та телекомунікаційної системи характеристики джиттера значень економічного BDS-тесту, а як критерій оцінювання – процентне відхилення наведеного показника від обраних в результаті експерименту значень.

Ключові слова: *комп'ютерні та телекомунікаційні системи; аномальна поведінка; BDS-тест.*

Рис. 5. Літ. 10.

Сергей Г. Семенов, Светлана Ю. Гавриленко, Виктор В. Челак

РАЗРАБОТКА ПАРАМЕТРИЧЕСКОГО КРИТЕРИЯ РЕГИСТРАЦИИ АНОМАЛЬНОГО ПОВЕДЕНИЯ КОМПЬЮТЕРНЫХ И ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ НА ОСНОВЕ ЭКОНОМИЧЕСКИХ ТЕСТОВ

В статье исследованы методы обнаружения злоумышленных атак на компьютерные и телекоммуникационные системы. Выявлена необходимость усовершенствования моделей информационных технологий и аргументированного выбора критериев оценки аномального поведения компьютерных и телекоммуникационных систем. Доказана целесообразность использования в качестве показателя аномального поведения компьютерной и телекоммуникационной системы характеристики джиттера значений экономического BDS-теста, а как критерий оценки – процентное отклонение приведенного показателя от выбранных в результате эксперимента значений.

Ключевые слова: *компьютерные и телекоммуникационные системы; аномальное поведение; BDS-тест.*

[1] National Technical University "Kharkiv Polytechnic Institute", Ukraine.
[2] National Technical University "Kharkiv Polytechnic Institute", Ukraine.
[3] National Technical University "Kharkiv Polytechnic Institute", Ukraine.

Problem statement. A typical feature of contemporary development of the society is information integration into the global world system, which is based on the use of computer and telecommunication tools everywhere. Under these conditions, the security of information resources from unsanctioned malicious actions and influence of computer viruses and other vicious software is a vital task. The issue is especially topical when solving economic security problems because if the information component is broken it can lead to severe financial and other losses (decrease in earnings, compromising sources, violation of commercial secret etc.).

When solving the problems related to diagnostics and security of computer information resources, the central task is timely detection of abnormal behavior in computer systems under the conditions of a virus attack.

Literature analysis (Brock et al., 1999; Goshko, 2009; Snow, 2002) shows that a variety of specialized antivirus systems based on signature and heuristics analysis is used to detect virus attacks. K. Kasperskiy (2006) shows that the signature method is based on comparison, where virus is matched with a particular signature or mask. The mask contains a number of malicious commands. A fragment of code, typical for this kind of virus, for example, a fragment of event trapping is often used as a signature.

The benefits of signature methods are the high level of malicious software detection and small percentage of false alarms. The flaws of this method include the inability to identify new, polymorphic and modified viruses. Additionally, signature analysis requires constant update of the database.

The main disadvantage of signature methods in detecting virus attacks is related to the inability of the system to detect attacks of unknown, as well as polymorphic and modified viruses, this can be eliminated by implementing heuristic methods of detecting anomalies in computer systems. The conducted research showed that the heuristic method imitates the process of human thinking. Implementing heuristic analysis allows us making a conclusion about the possible presence of a virus in the program.

As a result of the work of the heuristic method, it is not the code of the suspicious file that is analyzed, but rather its actions. A virus can copy its body into the memory, open other files and save its body there, save data to sectors of a hard drive, save or delete data from the key registry etc. The main disadvantage of the heuristics method is high percentage of false alarms.

The conducted research showed that the main way to eliminate the bottlenecks is to upgrade the models of information technologies and substantiate the choice of criteria in assessing abnormal behavior in computer and telecommunication systems.

The conducted research and literature analysis showed that a range of parametrical criteria are the base for various methods of anomaly detection (online – offline, Bayes – non-Bayes, parametrical – non-parametrical, known – unknown changes etc.) are used as criteria for assessing abnormal behavior in computer systems by heuristic analyzers.

It is worth mentioning that parametrical methods have more opportunities than non-parametrical ones. They allow detecting "true anomalies" under the conditions of fulfilling the criteria for the probability of false alarm detection.

The conducted experiments showed that the practical solution for the majority of parametrical methods for statistical detection of anomalies in computer systems

can be found by using the control chart method. Control charts can be applied to both numbers as well as alternative data.

The analysis of international standards (Kazarin, 2003; Snow, 2002) showed that control charts (for example, Shukhart's control charts, CUSUM-charts, charts of exponentially weighted moving average, moving average charts etc.) can be used to solve the problems (Brock et al., 1987). In this case, generally speaking, the more input data (indicators) is available for analysis, the more precise will be the result of assessment. However, should the model or assessment criteria be chosen wrongly, the parametrical methods lose their key advantages, thus leading to an increased number of false alarms.

Therefore, the conducted analysis of the existing approaches to antivirus data security showed the necessity of an adequate choice of abnormal behavior indicators in computer systems under the conditions of external input and the development of grading criteria, according to the chosen indicator.

Key results. The conducted analysis showed that one of the ways of parametrical analysis, which has great potential is *BDS-testing.* BDS-tests, suggested as a result of the analysis of finance markets by economists B. Brock, W. Dechert and J. Scheinkman in 1987, are effective methods for detecting the correspondences in timelines and their non-linear analysis. Their goal is to differentiate I.I.D. data and any form of functional connection to check the 0-th hypothesis H_0 for independence and equal assignment of values for dynamic series $\vec{\xi} = (\xi_1, \xi_2, \ldots, \xi_N)$, using the importance criteria for this. According to this criteria, to accept the H_0 hypothesis it is necessary to select the critical area G_α, which fulfills the condition $P(g \in G) = \alpha$, where $g(\xi_1, \xi_2, \ldots, \xi_N)$ is observation statistics, and α is the selected level of importance.

From (Uiler and Chambers, 2009) we know that the BDS-test is based on the statistic value $w(\vec{\xi})$ (BDS-statistics). The fundamental principles of mathematical formal characterization of the BDS-testing technology as applied in informational security facilities in computer systems are presented in (Semenov et al., 2010). The methods of structural identification of informational flows in telecommunication networks are examined in them. In the mentioned sources, the boundary value of BDS-test $|w_{m,N}(\varepsilon)| \le 1.96$ is used as the main criteria for abnormal behavior in computer systems (Brock et al., 1987; Kostenko et al., 2009). At the same time, the conducted research showed that this criteria does not fully reflect the results of virus attack influence on the aforementioned statistical indicators. Let us examine the results of virus attacks on computer system on practical examples.

To find the possibilities and particular qualities of a computer system state's identification under virus attacks, a imitational model was developed, and its input data was the value of CPU usage.

The model provides for the variation in the number of values in the dynamic series N. The value of CPU usage is scanned every second and is saved in a file.

The received values of CPU usage are divided into the samples of 500 values and are sent to the input of the analysis module, which is subjected to further processing and analysis with the help of BDS-statistics.

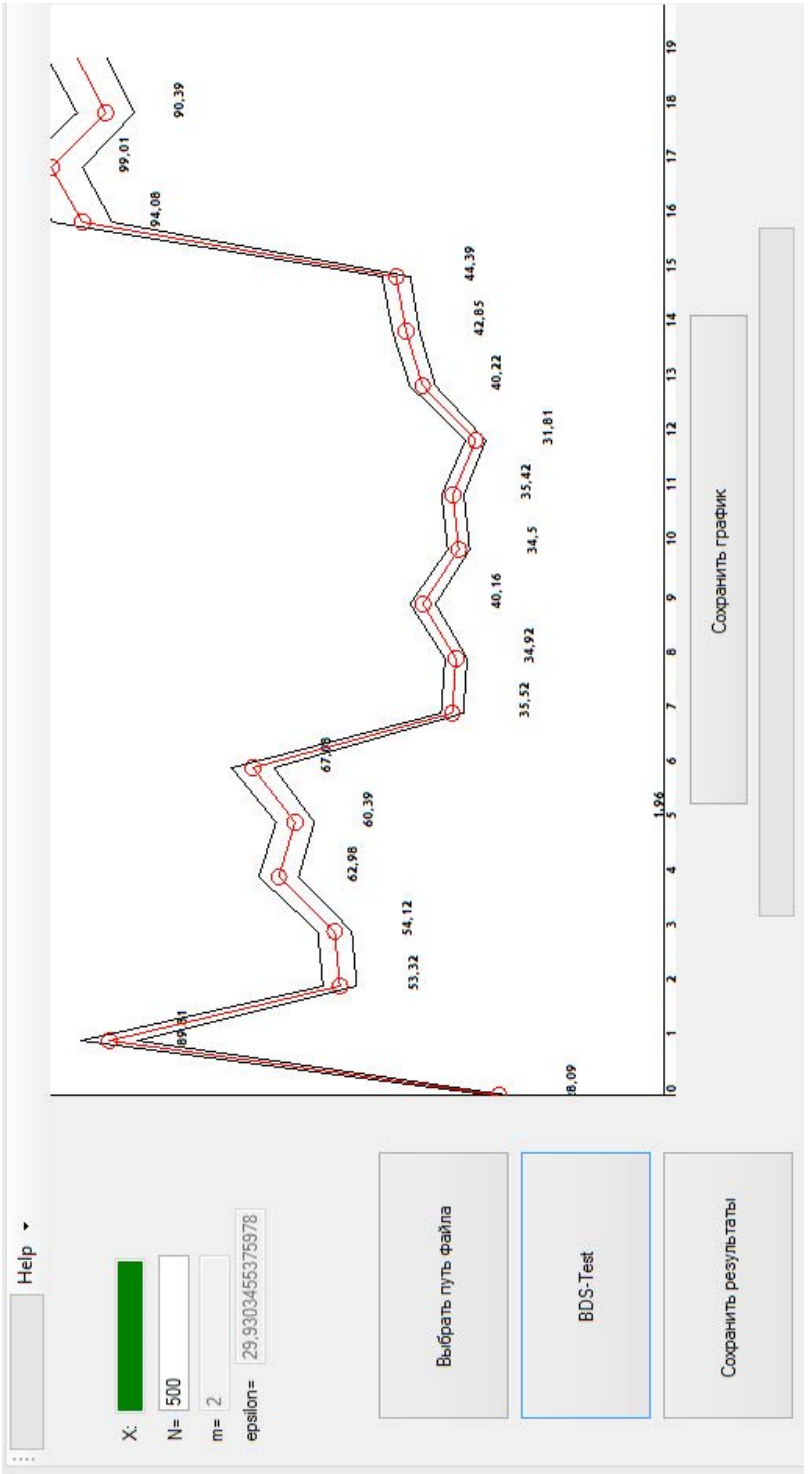

Figure 1. **Chart of BDS-test values during usual CPU usage in the "User" mode**, *authors'*

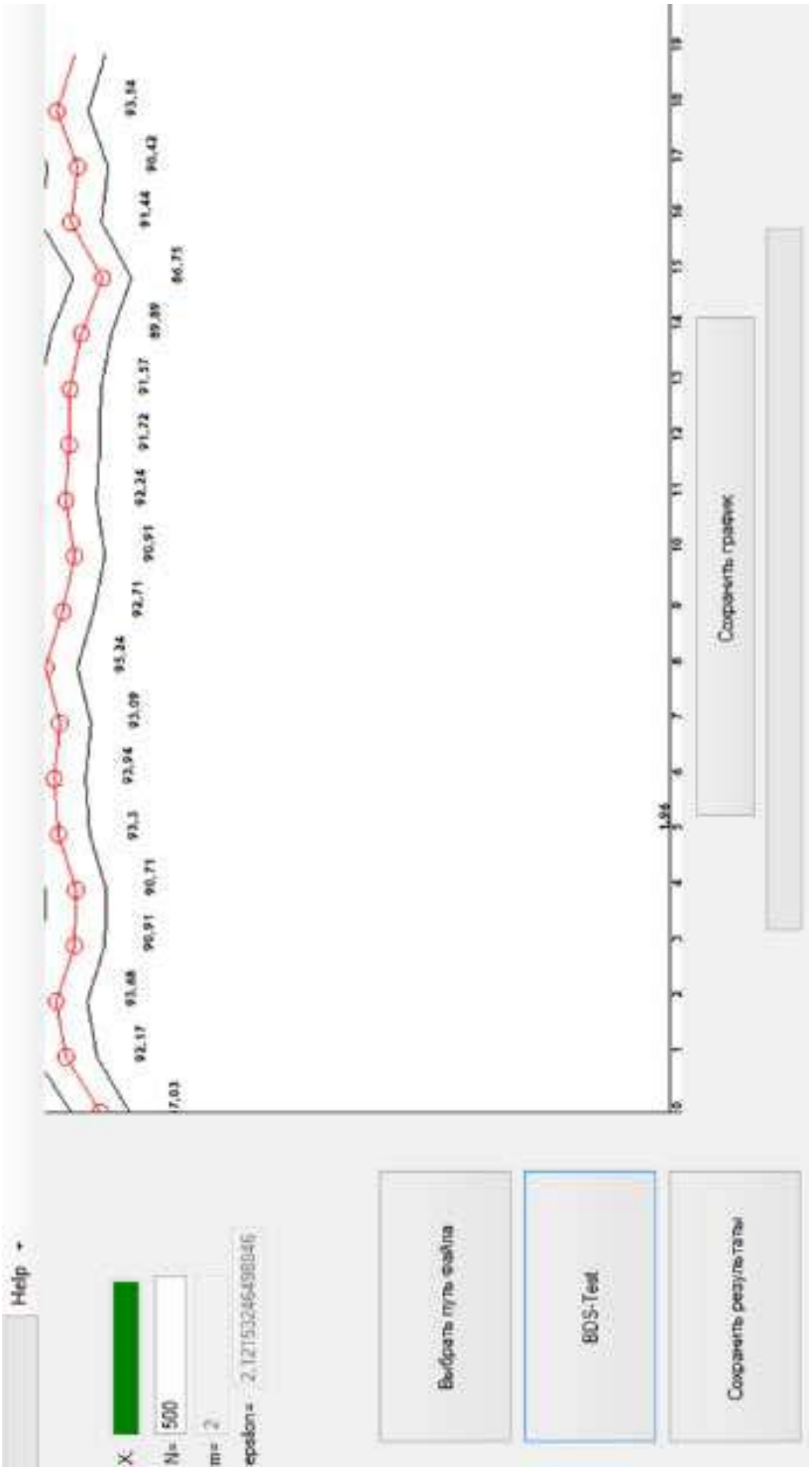

Figure 2. **Chart of BDS-test values during the computer's infection with the Svchost.exe virus**, *authors'*

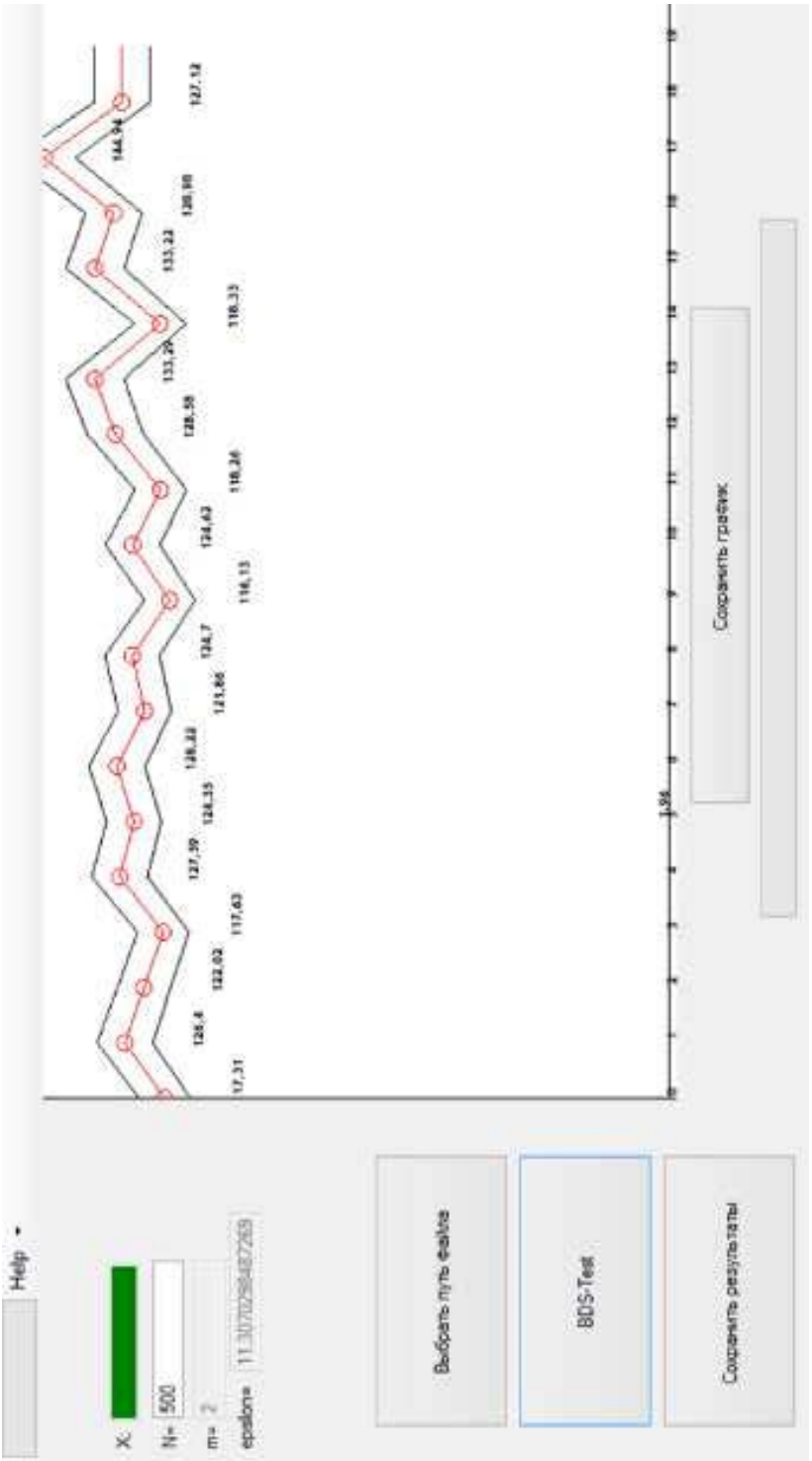

Figure 3. **BDS-test values after the computer's infection by the KillProc computer virus**, *authors'*

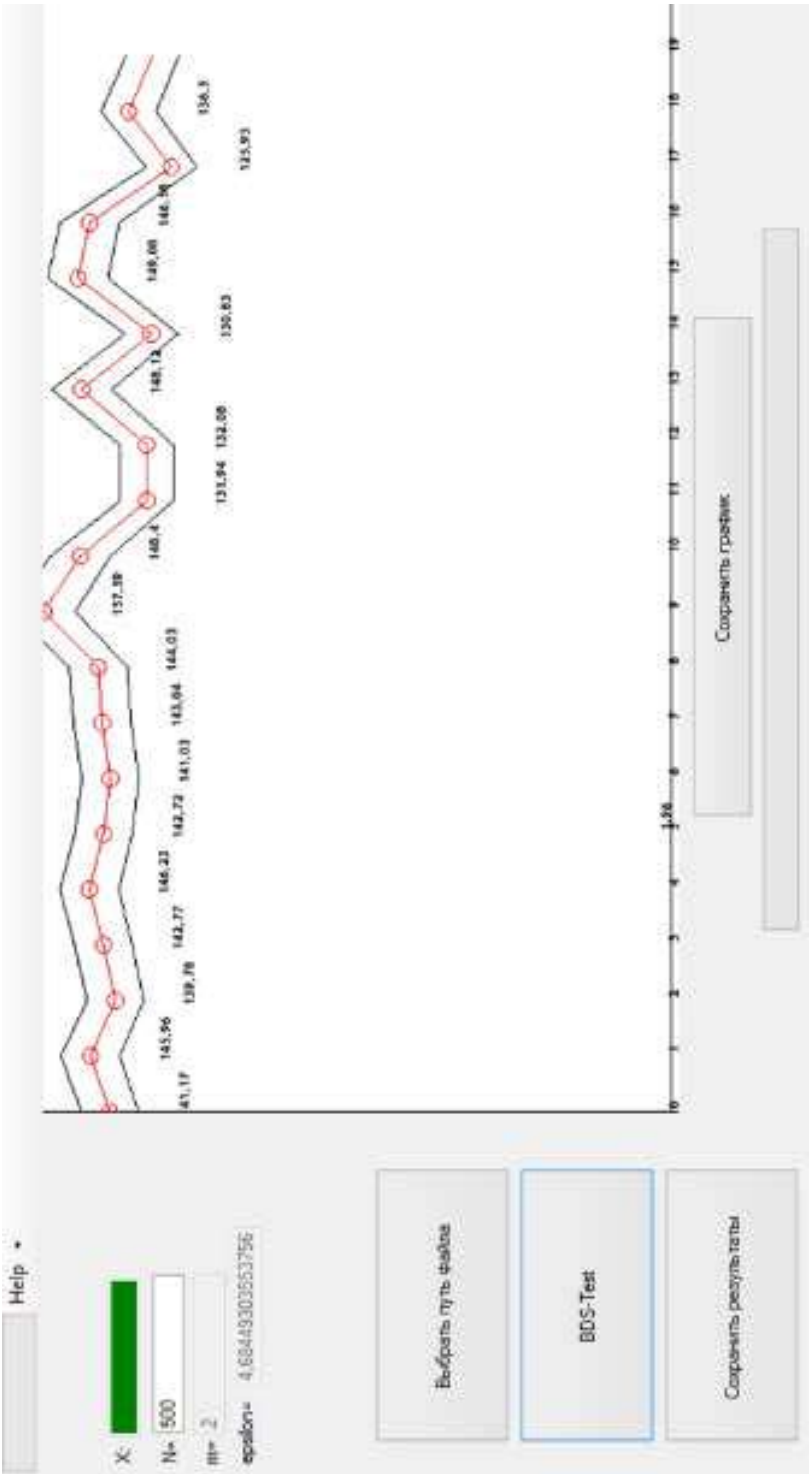

Figure 4. **BDS-test values after the computer's infection by the Kb657048.crs computer virus**, *authors'*

The result of the program model's work is $N/500$ values of the BDS-test.

Figure 1 shows the chart of BDS-test values during usual CPU usage in the "User" mode. The chart demonstrates that the minimal value of the BDS-value is close to 28, and the maximum value grows up to 99. Therefore, the maximum value of the BDS-test is 3 times as big as the minimal value, and the jitter (the difference between the maximum and the minimum) of the values reaches up to 70%.

Figure 2 shows BDS-test values during the computer's infection with the Svchost.exe virus (svchost.exe is a safe system process in Microsoft Windows, which is called the "Generic Host Process").

As we can see on the chart, the minimum value of the BDS-test is close to 77, and the maximum value reaches up to 95. Therefore, the jitter is brought down to 19%. This fact can become the signal for possible infection of the computer system by malicious software.

Similar results are deduced in an experiment, during the computer's infection with the *KillProc* (Figure 3) and *Kb657048.crs* computer viruses (Figure 4).

In the first case, the jitter between the maximum and minimum values is not bigger than 20%, the second case – no more that 19%.

The conducted research showed that a variety of viruses lead to a significant CPU usage growth. To prove this hypothesis, malicious software, imitating the work of a fork-bomb in Windows OS, was created.

The received temporal characteristics of CPU were processed with the help of BDS-test. The results are shown in Figure 5.

N	BDS-test values at infection fork-bomb
0	23,38
1	22,45
2	tends to infinity
3	tends to infinity
4	tends to infinity
5	tends to infinity
6	22,45
7	tends to infinity
8	tends to infinity
9	tends to infinity
10	tends to infinity
11	tends to infinity
12	tends to infinity
13	tends to infinity
14	tends to infinity
15	tends to infinity
16	tends to infinity
17	tends to infinity
18	22,55
19	22,45

Figure 5. **Analysis results, processed by a linear program**

As we can see in the experiment results, in the case of an infection of the computer system by a fork-bomb, the values of BDS-test tends to infinity in most of the cases, this can be a signal of infection of the computer system by malicious software.

Conclusions. Analysis and investigation of major economic security threats proved the topicality of antivirus data protection. Economic tests discovered a num-

ber of regularities which let us make a conclusion that the usage of one of them (BDS-test) is relevant if there exists aberrant behavior (computer virus) in the system. The conducted experiments showed the possibility of using the jitter characteristic of the BDS-test as an indicator of abnormal behavior in computer systems. The grading criteria is the deviation percentage of the shown value from the ones chosen as a result of an experiment with the values (20–70%).

The received results can be used in planning and implementing preventing measures and detecting outside perturbations of the computer system. This will ensure the exclusion of faults in the information sector of the economic system, which can lead to serious financial and other consequences.

References:

Гошко С.В. Технологии борьбы с компьютерными вирусами. – М.: Солон-Пресс, 2009. – 352 .

Казарин О.В. Безопасность программного обеспечения компьютерных систем. – М.: МГУЛ, 2003. – 212 с.

Касперский К. Записки исследователя компьютерных вирусов. – СПб.: Питер, 2006. – 316 с.

Семенов С.Г., Кузнецов О.О., Симоненко С.М., Мелешко Є.В. Метод структурной идентификации информационных потоков в телекоммуникационных сетях на основе BDS-тестирования // Наука і техніка повітряних сил Збройних сил України.– 2010.– Вип. 2. – С. 131–136.

Семенов С.Г., Смірнов О.А., Мелешко Є.В. Метод идентификации телекоммуникационного трафика на основе BDS-тестирования // Інформаційні технології в навігації і управлінні: стан та перспективи розвитку: Мат-лы наук.-техн. конф. – К.: ДП ЦНДІ НіУ, 2010. – С. 27–29.

Сноу Дж. Вирус на блюдечке // xakep.ru.

Уилер Д., Чамберс Д. Статистическое управление процессами: Оптимизация бизнеса с использованием контрольных карт. – М.: Альпина Паблишер, 2009. – 310 с.

Brock, W., Dechert, W., Scheinkman, J. (1987). Test for independence based on correlation dimension. Working Paper, University of Wisconsin, USA. Pp. 197–235.

Brock, W., Hsieh, D., LeBaron, B. (1999). Non-linear Dynamics, Chaos, and Instability. Cambridge, Massachusetts: The MIT Press, USA.

Kostenko, P.Yu., Barsukov, A.N., Vasiuta, K.S. (2009). Detection of the chaotic process distorted by the white noise using BDS statistics. Radioelectronics and Communications Systems, 52(11): 599–605.

Стаття надійшла до редакції 30.10.2015.