Quantitative Valuation of the Effectiveness of Existing Antivirus Software

Tatiana Markina
Saint Petersburg National Research University of Information Technologies, Mechanics and Optics
Saint Petersburg, Russian Federation
markina@cs.ifmo.ru, tmark812@mail.ru

***Abstract*—The article considers the existing methods of evaluating antivirus software. The paper proposes a method and model of estimation of the effectiveness of existing anti-virus protection. We examined the effectiveness of using anti-virus signature databases, heuristics or malicious behavior. A quantitative assessment of the existing means of protection against malicious software is described in paper.**

I. INTRODUCTION

Antivirus software is used for detecting and then preventing or removing malicious programs (malware). For most opinions antivirus doesn't offer a perfect solution to the problem of malware, but it is a critical first step to securing PC. To help prevent malware infecting PC you must install antivirus, and then regularly update your antivirus software.

Anti-virus protection – decisions based on an analysis of any monitored events to find a certain standard set (for example, signature and/or behavioral analysis). Because these reference sets cannot be complete, vulnerability created in the system is always detected only with a certain probability, which is depended on the completeness of the standard set of events.

In recent years, the technology that powers antivirus software has changed dramatically. An antivirus program that purchased a few years ago was able to stop known malware, but much harder to detect completely new and unknown malware. Newer products do a better job of stopping their spread.

Malicious programs are evolving faster than ever. Some sellers think that the latest generation of antivirus is better equipped than first of them to handle some new threats.

Back in 2009, experts have made the prediction for growth of virus activity. See Fig. 1, which resulted in the conclusion to the effect that in the coming years viral activity will only increase significantly, and in 2015 the number of new malicious programs could exceed 200 million [1]. Based on this forecast, that is based on the identification of the respective trend in [1] made another much more important conclusion about the technological dead end of the existing anti-virus protection technologies, in particular the need for a fundamentally different technologies to protect against malware.

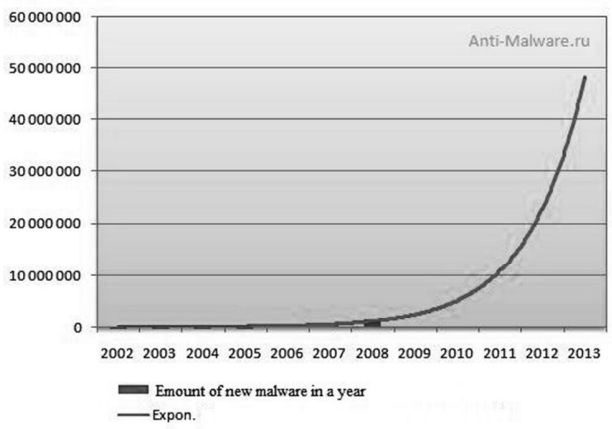

Fig. 1. The forecast increase in the number of malicious programs until 2013

Unfortunately, over the years, new technologies anti-virus protection (at least in wide use) has not appeared. Let's rate (after seven years), how this forecast is justified. Experts from the IB-Panda Security company published a report on cyber threats in the first quarter of 2013 [2]. According to the document, the specified period is a record in the number of malicious programs created daily. Thus, according to experts, in the first quarter were more than 15 million of new malware samples, the number of created malicious software was approximately 160 thousand per day. As you can see, the forecast is largely justified.

According to the most optimistic forecasts of the modern anti-virus protection equipment detected 75% of new malware, and the intensity of the creation of new malicious programs, as shown above, is determined by the dozens, if not already hundreds of millions a year.

There is another key problem of the anti-virus protection, which should be mentioned. Naturally, that the amount of signatures database grows in proportion to the growth of new detected malware. To check a file for a virus or for potential malicious activity, you must to compare this file for a match with any conditions (for example, before trying to execute, when recording to a computer, etc.) and with all signatures in the database. Naturally, this has an impact on a considerable load of computing resource, and this loading will be the bigger the greater the volume signature, and the rapid growth of the number of new malware created every day, we have illustrated.

ISSN 2305-7254

Of course, it is high time to think about the technological dead end of the existing antivirus protection technologies and look for new protection technology.

II. BEST ANTIVIRUS REVIEWS

You can easily find a lot of review about effectiveness of antivirus programs [3, 4]. They spoke about free and funded antivirus, about different operations system. If you open them, you will see that we have no problems with malware, but that's not the case.

The results reported by the independent antivirus programs testing laboratories were taken seriously. The simple fact is that a particular vendor's product that appears in the results is a sign of confidence. It means the laboratory considered the product significant, and the vendor felt the cost of testing was worthwhile.

There are a lot of series of test for antivirus programs. The best laboratories are West Coast Labs, Virus Bulletin, ICSA Labs, Dennis Technology Labs, AV-Test Institute (AV-Test.org), and AV-Comparatives (av-comparatives.org) [5].

Tests by the first three are based on simple threat-recognition, while the last three attempt to simulate real-world malware-attack scenarios.

AV-Test, one of the two leading antivirus testing houses, released its February antivirus ratings for Windows 8.1 PCs, assessing the 27 or so available antimalware packages on protection, performance, and usability. The results shouldn't surprise you: The bigger names in the industry rose to the top, while at the bottom sat Microsoft.

The team of AV-Test is a respected independent security-software testing lab based in Germany. AV-Test rigorously tests antivirus products from a number of leading security companies. The multifaceted testing procedure looks not only at how well an antivirus product can detect malware using traditional, largely signature-based methods (that is, employing a database of known malware types), but also at how well it can block brand-new, unknown malware. AV-Test also examines how well a security product can clean up after an infection in the event that a piece of malware does get through.

This tests focus on paid and free antivirus products. Paid antivirus products usually offer better technical support and more comprehensive protection features than free programs. Internet security suites go further still, offering firewalls, parental controls, identity theft protection and more.

The trouble is that some antivirus is better than others. They all offer a blacklist of known threats, and a whitelist of software that is known to be legitimate. But these days' new threats emerge every day, and knowing what is malware and what is not in real-time can be critical. AV-Test challenges Windows security software to withstand threats both: old and new, known and unknown.

Also the team of AV-Test test antivirus programs for how much (if at all) they slow down PC, as well as how easy to use and how intrusive they are. Thus you can see from AV-Test regularly updated list of the best antivirus for PC, which is the best for you. Best antivirus for protection, best antivirus for performance, and best antivirus for value.

The tests didn't just measure how effective each was in protecting PC from malware of all types; two-thirds of the score assessed how the software performed, and how usable it was. In the latter category, Microsoft scored a perfect six out of six – but so did eleven other vendors, showing how simple most antivirus software is to use.

AV-Test posted its results on antivirus and antimalware software for Windows 8.1 machines (Fig. 2) [6]. Microsoft's built-in antivirus came in last.

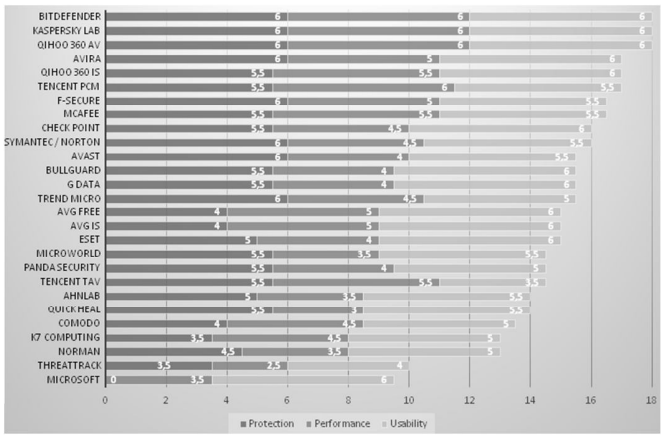

Fig. 2. The Best Virus Protection for Windows 8.1 – AV – TEST, January/February 2015

Another big laboratory is AV-Comparatives [7]. They use every security suite with its default settings. Their Whole-Product Dynamic Protection Test aims to simulate real-world conditions as experienced every day by users. If the user interactions are shown, they choose "Allow" or equivalent. If the product protects the system anyway, they count the malware as blocked, even though they allow the program to run when the user is asked to make a decision. If the system is compromised, they count it as user-dependent. They consider "protection" to mean that the system is not compromised. This means that the malware is not running (or is removed/terminated) and there are no significant/malicious system changes. An outbound-firewall alert about a running malware process, which asks whether or not to block traffic from the users' workstation to the Internet, is too little, too late and not considered by us to be protection.

Then they every morning, any available security software updates are downloaded and installed, and a new base image is made for that day. Before each test case is carried out, the products have some time to download and install newer updates which have just been released, as well as to load their protection modules (which in several cases takes some minutes). In the event that a major signature update for a product is made available during the day, but fails to download/install before each test case starts, the product will at least have the signatures that were available at the start of the day. This replicates the situation of an ordinary user in the real world.

AV-Comparatives told that security products should protect the user's PC and it is not very important at which stage the protection takes place. They test if it is protected while browsing to the website (e.g. protection through URL Blocker), while an exploit tries to run, while the file is being downloaded/created or when the malware is executed (either by the exploit or by the user). After the malware is executed (if not blocked before), they wait several minutes for malicious actions and also to give e.g. behavior-blockers time to react and remedy actions performed by the malware. If the malware is not detected and the system is indeed infected/compromised, the process goes to "System Compromised". If a user interaction is required and it is up to the user to decide if something is malicious, and in the case of the worst user decision the system gets compromised, they rate this as "user-dependent". Because of this, the yellow bars in the results graph can be interpreted either as protected or not protected (it's up to each individual user to decide what he/she would probably do in that situation).

AV-Comparatives laboratory aim to use visible and relevant malicious websites/malware that is currently out there, and present a risk to ordinary users. They usually try to include as many working drive-by exploits as they find – these are usually well covered by practically all major security products, which may be one reason why the scores look relatively high. The rest are URLs that point directly to malware executable; this causes the malware file to be downloaded, thus replicating a scenario in which the user is tricked by social engineering into following links in spam mails or websites, or installing some Trojan or other malicious software.

As you can see all such laboratories use test cases – set of malware programs. So it cannot show us how efficient antivirus programs are when using them for protection against new malware programs.

III. MODEL OF THE CALCULATION OF THE EFFICIENCY

To quantify the effectiveness of antimalware programs we may use the model that is described below. In this paper it is considered the effectiveness of antivirus software using signature databases, heuristics or malicious behavior.

For a quantitative evaluation of the existing protection methods we constructed a mathematical model. We represent the discovery of a new malicious program as a queuing system [8], [9], [10], [11], [12], [13], where the server is the analyst (or sometimes program for analysis); the customer (arrival) is the new malware. In the result it is a multi-server queuing model with unlimited queue M/M/C.

We offer a mathematical model for the calculation of the efficiency that can be built depending on the tasks:

$$p_0 = f(\lambda, \mu), \tag{1}$$

where p_0 – the probability of n customers in system, λ – the average arrival rate, μ – the average service rate.

Under the average arrival rate we understand the intensity of detection of new malicious programs. Under the average service rate we understand the intensity of releasing new signatures and heuristics. These values are defined on the basis of the existing statistics.

IV. CALCULATION OF EFFICIENCY

Consider the stationary operation of the system:

$$\frac{\rho}{C} < 1, \tag{2}$$

where ρ – server utilization, equal to the ratio of average arrival rate to the average service rate:

$$\rho = \frac{\lambda}{\mu} \tag{3}$$

C – the number of parallel servers.

Using the formula (2) and (3), we obtain the inequality:

$$\frac{\lambda}{\mu * C} < 1 \tag{4}$$

The average service rate and the number of servers we set on the basis of general information on the work of anti-virus companies.

If we will know these parameters, we can obtain from (4) interval. It limits the average arrival rate in a stationary distribution:

$$\lambda < \mu * C \tag{5}$$

Suppose that all received on the analysis programs are malicious and unique. We will consider only those programs (customers), the result of the processing of which was the addition of a signature. Analysis of the program includes: decompile, progressive learning, selection of signature.

Assume that the analysis program (average time spent by a customer from arrival until fully served) is 10 min, 30 min and 60 min. This assumption is based on data about the frequency of updates are released, for example, Symantec publishes new bases with a frequency of 15 minutes (pulse updates) [14], and the Kaspersky Lab company – with a frequency of 2 hours [15].

Consider the situation when 100 and 1000 analysts work.

1) Consider the first case:

$C = 100$ $T_r = 10$ min ($\mu = 0.1$)

From the formula (5) we can say that if the system should works in a stationary mode, the average arrival rate (λ) must be less than 10.

In the first place we should calculate the probability (p_0) that all analysts will be free and there will not new customers (arrivals). The probability p_0 is the characteristic urgency of a

threat. The less the probability p_0 is then more actual the threat is. The probability p_0 that the system is ready for use at any time and no signature is not detected, is calculated by the formula:

$$p_0 = \left(\sum_{n=0}^{C} \frac{p^n}{n!} + \frac{\rho^{C+1}}{C!\,(C - \frac{\lambda}{\mu})}\right)^{-1} \quad (6)$$

Let's calculate p_0 for λ given in Table I.

TABLE I. P_0 CALCULATE WITH DIFFERENT Λ

λ	1	1.2	1.3	1.4	1.5	1.7	2
p_0	5E-05	6.14E-06	2.26E-06	8.32E-07	3.00E-07	4.14E-08	2E-09

λ	3	5	6	7	8	9
p_0	9.4E-14	1.93E-22	8.80E-27	3.98E-31	1.80E-35	7.60E-40

Fig. 3 shows a dependence of λ to p_0.

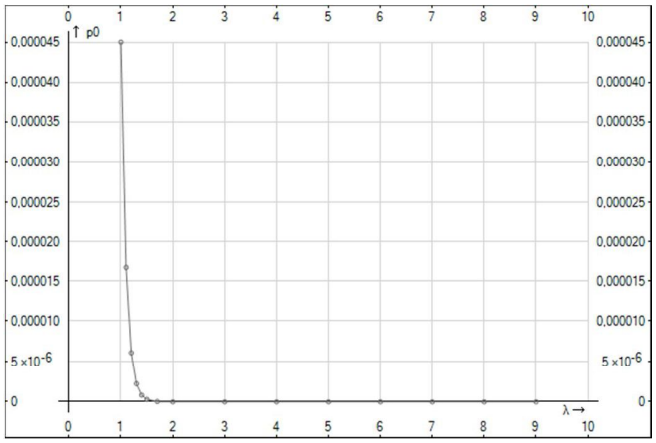

Fig. 3. The dependence of the intensity of the applications received from the probability p_0

The graph (Fig. 3) demonstrated that an increase in the intensity of the applications received in the QS, the likelihood that the system does not will a single application, tends to zero.

2) Considering other conditions, we get similar graphs as shown in Fig. 3.

The calculated values are shown in Tables II.

As a result of research we find that the subject in 1000 of servers (analysts) and service time of 60 minutes, increasing the intensity of the condition of receipt of applications in the absence of likelihood of employment instruments falling sharply.

Analysis calculated performance shows a significant overload of nodes in the presence of the calculation of the number of analysts and service time applications.

TABLE II. THE PROBABILITY THAT ALL ANALYSTS WILL BE FREE DEPENDING ON AVERAGE RATE OF NEW MALWARE

C = 100; T_r = 60 min; μ = 0.01(6)					
λ, min^{-1}	0.1	0.1375	0.17	0.2	0.3
p_0	0.00245	0.00026	0.00012	6.144E-06	1.523E-08
λ, min^{-1}	0.5	1.1	1.3	1.5	1.66
p_0	9.36E-14	2.17E-29	1.33E-34	7.62E-40	2.25E-44
C = 1000; T_r = 10 min; μ = 0.1					
λ, min^{-1}	10	10.5	14	20	30
p_0	3.72E-44	2.51E-46	1.58E-61	1.38E-87	5.15E-131
λ, min^{-1}	40	60	70	80	90
p_0	1.90E-174	2.65E-261	9.86E-305	3.67E-349	1.36E-390
C = 1000; T_r = 30 min; μ = 0.0(3)					
λ, min^{-1}	1	1.1	2	3	4
p_0	9.36E-14	4.66E-15	8.76E-27	8.19E-40	7.67E-53
λ, min^{-1}	5	9	17	21	
p_0	7.18E-66	5.50E-118	3.23E-222	2.48E-274	
C = 1000; T_r = 60 min; μ = 0.01(6)					
λ, min^{-1}	0.5	0.55	0.75	1	1.5
p_0	9.35E-14	4.66E-15	2.86E-20	8.76E-27	8.19E-40
λ, min^{-1}	2	4.5	6.5	8.5	10.5
p_0	7.67E-53	5.50E-118	4.22E-170	3.23E-222	2.48E-274

V. MAIN CALCULATIONS

Earlier versions were discussed with the task QS service time and the number of devices, the intensity of receiving applications was taken on the basis of the conditions of stationary operation of the system. Now consider what should be the time of service in the case of known intensity receipt of applications, in other words, the intensity of the emergence of new malware.

Every year, publishes the number of detected new malicious programs – the number of signatures added. Based on these values, we can calculate what should be a time of service applications.

Forecast laboratory Anti-Malware on the increase in the number of new malicious programs [16] is shown in Fig. 1. According to the reports for 2013 [17], [18], [19] this prediction came true.

According to a report [2] for the third quarter of 2013 for the period it was found about 10 million new malware (signature). Based on this figure, the intensity of the receipt of applications is found to be 77.15 Applications/min. Suppose that 100, 1000, 2500 and 5000 analysts work. Number of

employees, for example, in Kaspersky Lab is more than 2800 people [20], but this figure includes not only the analysts.

We calculate what will be the length of the queue on the basis of the statistical rate of receipt of applications. Consider the case of steady-state operation of the system:

$$\frac{\rho}{C} < 1 \tag{7}$$

It follows from (7) and (3), we obtain:

$$\mu < \frac{\lambda}{C} \tag{8}$$

Knowing that $\mu = 1/T_r$, we obtain from (7) restrictions on the average service time application:

$$T_r < \frac{\lambda}{C} \tag{9}$$

Based on (5) we ask T_r and calculate the average queue length according to the formula:

$$L_r = \frac{\rho^{C+1}\rho_0}{C * C!\,(1 - {}^{\rho}/_{C})^2} \tag{10}$$

The obtained values are presented in Table III.

TABLE III T_r AND L_r DEPENDING ON C

1) C = 100; T_r < 1.296 min							
T_r, min	0.9	1.2	1.23	1.26	1.28	1.29	1.295 (9)
L_r	0.0008	4.29	9.26	24.26	67.67	196.94	7339.75
2) C = 1000; T_r < 12.96 min							
T_r, min	5	12	12.5	12.6	12.8	12.9	12.95 (9)
L_r	1.5E-149	0.12	4.74	9.5	46.66	172.28	7312.74
3) C = 2500; T_r < 32.405 min							
T_r, min	14	31	31.5	32	32.2	32.3	32.4
L_r	3.12E-297	0.36	3.6	33.05	103.88	251.58	7289.86
4) C = 5000; T_r < 64.81 min							
T_r, min	32	63	63.5	64	64.4	64.6	64.8
L_r	7.98E-489	0.96	4.71	21.64	86.14	230.04	7264.27

We will introduce the dependence of the average queue length of the average service time applications (Fig. 4).

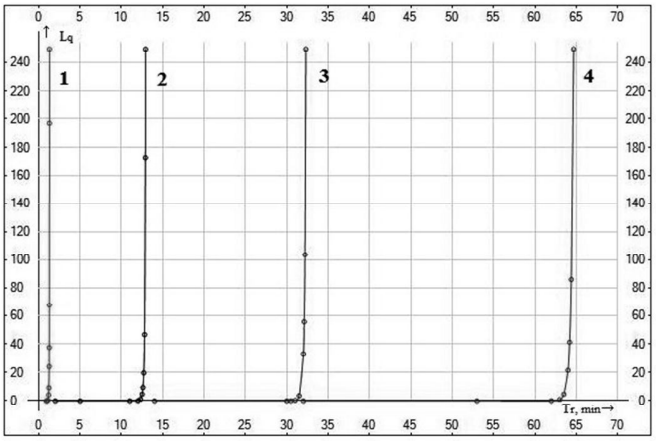

Fig. 4. Graph of the average queue length of the average service time applications

Fig. 4 shows four graph of the average number of requests in the queue from the average service time. From the chart, we see that the system is close to the non-stationary. Based on the real-time service performance and intensity come first served, received a sharp increase in the length of queues and a corresponding time of service applications.

Studies have shown that if a system of servers in 1000, the steady state is achieved only when the service time is not more than 13 minutes, while the average queue length of 7300 applications. If the average time increased to 65 minutes, you must have 5000 service units, and the average queue length is approximately 7300 applications.

Now consider how long the application will wait in the queue if the service time close to critical for a given amount of servers and service rate. To this end, shall specify time limits for service up to 4-5 decimal places. Based on this setting, select the most close to the maximum and that the load on the channel was the highest.

Average service time of the application is calculated as follows:

$$T_q = \frac{L_q}{\lambda} \tag{11}$$

The results of calculations are presented in Table IV.

In view of the high intensity of detection of new malicious programs, QS, representing the work of antivirus software, should be considered in conditions close to the non-stationary (stationary on the border).

The studies find that in the case where the number of servers is 1000, and the average service time of a single application of 12.9616 minutes – the average queue length is equal to 79578.87 and the waiting time will be 1031.48 m. If the value of the average time of service just add 0.00009 min (5.4 ms), and the average length of waiting time will be doubled.

TABLE IV. THE AVERAGE SERVICE TIME OF THE APPLICATION

1. C = 100; T_r < 1.29617 min				
T_r, min	1,2959	1.295999	1.2961	1.29616(9)
λ/Cμ	0.9997	0.99986	0.9999	0.999995
L_q	4678.34	7298.27	16979.15	206387.1
T_q, min	60.64	94.6	220.08	2675.14
2. C = 1000; T_r < 12.9617 min				
T_r, min	12.959	12.961	12.9616	12.96169(9)
λ/Cμ	0.99979	0.99994	0.999987	0.9999995
L_q	4651.36	16952.25	79578.87	206409.72
T_q, min	60.29	219.73	1031.48	2675.44
3. C = 2500; T_r < 32.4044 min				
T_r, min	32.4	32.403	32.404	32.4043(9)
λ/Cμ	0.999864	0.999956	0.999996	0.9999996
L_q	7289.86	22969.3	79555.85	4675694.38
T_q, min	94.489	297.73	1031.19	60605.24
4. C = 5000; T_r < 64.8088 minutes				
T_r, min	64.8	64.808	64.8087	64.8087(9)
λ/Cμ	0.999864	0.999988	0.999998	0.9999998
L_q	7264.27	79529.91	569284.41	4675668.86
T_q, min	94.16	1030.85	7378.93	60604.91

In the case where the average service time of 64.808 min, taking into account the intensity of the applications received bids 77.15 per minute, the number of servers must be equal to 5000. In these conditions, the average queue length is equal to 79529.91 and the waiting time is 1030.85 min. If the average service time of applications increases on 0.0007 m (42 ms), the average queue length and waiting time will grow in 7 times.

If we consider the QS in the closest state to unsteady: C = 1000 = 12.96169 T_r (9) and C = 5000 T_r = 64.8087 (9), we see that in these conditions the system can be called non-stationary as impossible to implement the conditions obtained in practice.

As shown in the research, the effectiveness of anti-virus software should be evaluated not based the time of creating a new signature or intensity of service, but it should be based on the number of applications in the queue for service and the waiting time in the queue. If we assume that the system is operating in a stationary state, setting the average arrival rate of applications and the number of analysts, we will have a system close to a non-stationary as in the extreme points turn increases dramatically. This indicates a low effectiveness of existing anti-virus software and the lack of the required level of protection. All of this suggests the need for new approaches to the protection against malicious software.

VI. CONCLUSION

The quantitative valuation of the effectiveness of existing antivirus software was calculated. On current statistics show that the most urgent protection in modern threat systems implementation and launch a malicious program.

A mathematical model of a QS M/M/C is used to evaluate the effectiveness of existing methods and means of virus protection. In this model, to quantify the effectiveness of modern anti-virus tools. As a result, it is shown that if a system has 1000 servers, the stationary state is achieved in the case of service time no more than 13 minutes, while the average queue length is 7300 applications. If the average service time increased to 65 minutes, for stationary state you will need already 5000 servers (5000 virus analysts in the same company). As a result of the conclusion with respect to the fact that the QS, which describe the modeled system, should be considered in a non-stationary mode, for which all requests for services grows endlessly.

Simulation is performed in conditions close to the non-stationary to estimate the values of the basic characteristics of the QS – average waiting time in the queue for the application service and the average queue length. As a result of simulation obtained that, for example, if the average service time of the application (signature detection) is 64.808 minutes and the intensity of the receipt of applications is 77.15 applications per minute (the stationary system is achieved when the number of servers is equal to 5000), than the average queue length is equal to 79529.91, while the waiting time is 1030.85 min. If the average service time of applications will increased only on 0.0007 min (42 ms), the average queue length and waiting time will increase in 7 times.

As you can see, characteristic of the efficacy of anti-virus protection - the average time of service of the application (signature detection), that is used today in practice – does not reflect the real situation.

On the basis of the research concluded that the fundamental impossibility of building an effective protection against malicious software using known methods of protection, indicating the need to develop new approaches to protect, based on different principles, and new methods of protection against malicious software.

REFERENCES

[1] Analytical center Anti-Malware.ru official website, I. Shabanov, "Antivirus vendors looking out of the technological impasse", Web: http://www.antimalware.ru/antivirus_trends.

[2] PANDALABS official website, "Quarterly report PANDALABS July – September 2013", Web: http://www.viruslab.ru/upload/files/download/wp/wp_reports_2013.pdf.

[3] 10TopTenReviews official website, "Antivirus Software Reviews" , Web: http://anti-virus-software-review.toptenreviews.com/.

[4] PC ADVISOR official website, Matt Egan, "15 best antivirus & best free antivirus for PC and laptop UK: 2016's best antivirus for protection, performance value", Web: http://www.pcadvisor.co.uk/test-centre/security/best-antivirus-for-pc-laptop-2016-uk-free-3263332/.

[5] PCMag Digital Group official website, Neil J. Rubenking, "The Best Antivirus Utilities for 2016", Web: http://www.pcmag.com/article2/0,2817,2372364,00.asp.

[6] AV Test official website, "Test Results", Web: https://www.av-test.org/en/press/test-results/.

[7] AV-Comparatives official website, "Whole Product Dynamic «Real-World» Protection Test", Web: http://www.av-comparatives.org/wp-content/uploads/2015/12/avc_prot_2015b_en.pdf.

[8] N. N. Amosov, B. A. Kuklin, S. B. Makarov, *Stochastic mathematics: probability Theory. Mathematical statistics. Theory of*

*stochastic processes. Queuing theory. The textbook for Technical colleges,*St. Petersburg.: Ivan Fedorov, 2001.

[9] B. V. Gnedenko, I. N. Kovalenko, *Introduction to the theory of mass service,* Moscow: URSS Publ LCI, 2013.

[10] G. I. Ivchenko, *Queuing theory*, Moscow: URSS, 2012.

[11] G. P. Klimov, *Queuing Theory*, Moscow: Publishing house of Moscow University, 2011.

[12] A. A. Tarantsev, *Engineering methods of queuing theory,* St. Petersburg: Nauka, 2007.

[13] O. M. Tikhonenko, *Queuing modeling in information systems: textbook for Universities,* Minsk: Tehnoprint, 2003.

[14] Norton Internet Security official website, "Opportunities of Norton Internet Security", Web: https://support.norton.com/sp/ru/ru/home/current/solutions/v59829727_EndUserProfile_ru_ru?q=15минут.

[15] Kaspersky Lab official website, "The frequency with which updates are downloaded anti-virus databases if you select "Automatically" in the properties of the update task?", Web: http://support.kaspersky.ru/8595.

[16] Portal ISO27000 official website, S. Il'in, "Anti-virus vendors are seeking a way out of the technological impasse", Web: http://www.защита-информации.su/chitalnyi-zai/antivirusnaya-zaschita/antivirusnye-vendory-ischut-vyhod-iz-tehnologicheskogo-tupika.

[17] Verizon official website, "2013 DATA BREACH INVESTIGATIONS REPORT Verizon", Web: http://www.verizonenterprise.com/DBIR/2013/.

[18] Cisco official website, "Cisco 2014 Annual Security Report", Web: https://www.cisco.com/web/offer/gist_ty2_asset/Cisco_2014_ASR.pdf.

[19] Kaspersky Lab official website, "Kaspersky security bulletin 2013", Web: http://media.kaspersky.com/pdf/KSB_2013_RU.pdf.

[20] Kaspersky Lab official website, "About "Kaspersky Lab"", Web: http://www.kaspersky.ru/about.