Київський університет імені Бориса Грінченка 1874

КІБЕРБЕЗПЕКА: освіта, наука, техніка

CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE

№ 4 (4), 2019

ISSN 2663 - 4023

DOI 10.28925/2663-4023.2019.4..6271

UDC 004.056

Svitlana M. Shevchenko
Pnd, Associate Professor of Department of Computer Science and Mathematics
Borys Grinchenko Kyiv University, Kyiv, Ukraine
OrcID 0000-0002-9736-8623
s.shevchenko@kubg.edu.ua

Pavlo M. Skladannyi
Senior Lecturer of the Department of Information and Cyber Security
Borys Grinchenko Kyiv University, Kyiv, Ukraine
OrcID 0000-0002-7775-6039
p.skladannyi@kubg.edu.ua

Maksym Martseniuk
student of the Department of Information and Cyber Security
Borys Grinchenko Kyiv University, Kyiv, Ukraine
OrcID 0000-0002-6662-7610
msmartseniuk.fitu18@kubg.edu.ua

ANALYSIS AND RESEARCH OF THE CHARACTERISTICS OF STANDARDIZED IN UKRAINE ANTIVIRUS SOFTWARE

Annotation. The article is devoted to the problem of information security, namely the study of the characteristics of antivirus programs which are standardized in Ukraine. The study used statistical methods to analyze the characteristics of antivirus software and comparative methods of comparing the various types of such programs. Relying on researches in scientific literature, the main threats to information security in the field of information technology were analyzed. The emphasis is placed on the fact that antivirus software is the most effective protection against malicious software (malware). The basic methods of work of the antivirus – signature and heuristic – are described. The list of standardized in Ukraine antivirus programs is determined. The study was based on the quantitative and qualitative results which while testing had obtained by the independent testing laboratory AV-Comparatives (Austria), the independent Virus Bulletin (VB) laboratory for testing and certification in the field of security, the Center for antivirus protection information of the State Special Communication Service of Ukraine. The comparative analysis of the main characteristics of antivirus programs was carried out, namely: antivirus and anti-spyware; anti-phishing; anti-rootkit protection against exploits; Intrusion Prevention System; Real-time protection; parental control; host-based firewall; antispam; protection against network attacks; home network protection; anti-theft; password management.

Key words: antivirus software; information protection; characteristics of antivirus programs; malicious software (malware).

1. INTRODUCTION

Formulation of the problem. In our time of global computerization, with the growth of information technology and systems, malicious software (malware) raises and develops with the same pace, and even faster. Viral programs use our devices for network attacks and site hijacking, steal personal information or confidential documents. Cybercrimes inflicted $ 3 billion of damages in 2015, and by 2021 this figure will increase to 6 billion [1].

Cisco experts believe that malicious software brings malware to unprecedented levels of excellence and exposure, and increasingly avoid the detection and use cloud services and other technologies as their weapon that are commonly used for legal purposes [2]. Obviously, data security and data protection have become a key issue nowadays.

Analysis of recent research and publications. The works of V. Baranov, V. Baryachok, Y. Bogdanovich, V. Dudikevich, P. Balashov, A. Korchenko, N. Kazakova, S. Kazmirchuk, V. Horoshka, L. Hoffman, W. Jansen, D. Catteddu and other scientists of this field are devoted to the studying of the problem of resistance to breaking of information system, assessment of the state of security of information resources. The matters related to the development of antivirus software, the effective use of antivirus software and minimization of the effects of cyber threats, the on time detection and localization of computer viruses, were considered in the works of E. Kucher, P. Baudisch, E. Hopkins, E. Kaspersky, D. Lozynsky, K. Kaspersky, S. Smirnov. They are unanimous that antivirus software is the most effective mean of protection against threats to information security [3-7].

Virus engineering technologies are developing very fast. In 2018 around the world existed more than 750 million strains of malware, and 4 new ones are generated every second [8]. In this regard, antivirus programs tend to become obsolete. Therefore, updating information on this issue is always relevant.

The outlined above had shown the purpose of our study – to highlight the main characteristics of standardized antivirus programs in Ukraine, which will allow users to build the best possible perimeter of host-based and corporate information security.

2. THEORETICAL BASIS OF THE STUDY

Popularity, widespread distribution of the system; availability of diverse and sufficiently complete documentation about the system; vulnerability of the system or the existence of known vulnerabilities in the security system – are the conditions for the appearance of malware in a particular operating system or application, which should have simultaneous fulfilment. Malicious software includes programs that have received names such as: classic computer viruses, network worms, Trojans, hacker tools, and others. All of them cause either obvious damage to the computer where they are run on, or it damages other computers on the network, or performs other unauthorized actions. To actions which are not make direct harm are included the spam spreading, persistent advertising, transmission of confidential information to the attacker, and others.

Along with the complexity of viruses, antivirus programs become more and more complex. An antivirus software is a software that is designed to protect the objects / resources of information and telecommunication systems from damage caused by computer viruses [9]. The analysis of literature [3-7, 10] allowed to determine that at the present stage, specialists distinguish two main methods of work of antivirus programs: signature and heuristic.

Signature analyzer in interaction with a signature database detects known computer viruses through their specific code areas - masks or signatures. This analyzer implements a strategy of antivirus protection which should response to the methods that the authors of the virus have already developed. In another words, the essence of signature analyzer is the confrontation with certain computer viruses that are known and have been analyzed in detail. It also performs a polyphage function and can treat infected files (except when the latter were irreversibly distorted by a computer virus). However, the signature method has several disadvantages. The most important of them is the delay in responding to new threats. Signatures always appear only after some time since the virus appeared, while modern harmful codes in a very short time can infect millions of computers.

The heuristic analyzer, during its interaction with a base of heuristic features, detects known and unknown viruses, in terms of their characteristic features. It implements both existing antivirus protection strategies: prediction of methods that will be used by the authors of viruses in the future and responding to the methods that the virus authors have already developed. Heuristic method imitates the process of human thinking. In the course of the work the heuristic method analyzes not the code of the malicious program, but it actions. There are two methods of heuristic analyzers: static and dynamic. The static methods search for a short signals, because such signals are the most suspicious in malicious software. The advantage of this method is the ease implementation and high speed, but the level of detection of new malware is quite low. The dynamic heuristic analysis is sometimes marked out in a separate technology for detecting malicious software – which provides an analysis of the program behavior (or behavioral analysis). While using the dynamic analysis, the start of the program emulates in the virtual address space, and the decision about the nature of the object is taken on the basis of analysis of the actions performed by it. Often, this method checks scripts and macros, also it is possible to track an attempts of direct access to files, to format hard disks. If the heuristic analyzer displays suspicious activity during the emulation, then the program is considered harmful or suspicious, and its start on the user's computer is blocked [5].

Nowadays the list of the available antivirus programs is huge enough. They differ both in price (from fairly expensive-commercial to absolutely free), and in terms of its functional capabilities. However, it should be noted that none of the existed antivirus programs can provide 100% protection.

3. RESULTS OF THE STUDY

The following antivirus programs that are certified in Ukraine [11] were selected for this research and analysis of the characteristics of the antivirus software, namely:

1. Antivirus software “Avast”
2. Antivirus protection software “Sophos”
3. Antivirus software “Panzor Cloud Antivirus:
4. Symantec antivirus protection software
5. Antivirus protection software “Zillya”
6. Antivirus protection software “Eset”
7. McAfee Antivirus Protection Software
8. Bitdefender Information Resources Program
9. Program complex of information resources protection “Trend Micro”
10. Software product for protection against harmful software “ROMAD”

Our research is based on the results obtained in 2018 by the independent testing laboratory AV-Comparatives (Australia), which tests the antivirus software [12], the independent laboratory Virus Bulletin (VB) of testing and certifying in the field of security [13], the Antivirus Center Protection of information of the State Social Service of Ukraine [11]. The quantitative indicators you can check on the websites of the mentioned above laboratories.

3.1. Develper – **AVAST Software** (Czech Republic), 1988 [11, 13, 14-16]. It is the largest threat detection network, machine learning technology, the simple password and billing mechanism, and home network security provider with minimal system resources load. In 2018, it received the Advanced + Award in every test of that year. Also it gained a golden prize for a testing of protection against malware, a silver prize – for the removing malware, a bronze prize – for the performance test.

The software package of antivirus protection “avast! Endpoint Protection Suite Plus” version 8.X.Y in Ukraine manufactured by AVAST Software a.s. It provides information security of common PC or corporate networks through the multi-level protection of computer information resources from the penetration of harmful and potentially dangerous objects of any external sources. It responds to the requirements of reference documentation (RD) for technical information protection (TIP) in the scope of the functions specified in the document “Antivirus protection software “avast! Endpoint Protection Suite version 8.X.Y. The technical requirements for the protection of information from unauthorized access", the totality of which is determined by the functional profile.

3.2. Developer - **Sophos Group** (England), 1985 [11, 12, 17]. Sophos Enterprise Console is a free antivirus solution for personal use. Among the main benefits of this program can be counted an automatic antivirus protection, Web-based protection and Potentially Unwanted Programs (PUP) detection, as well as a massive list of 8 services that will be launched at Windows startup and run all the time. The main problem consists of that it is impossible to control the program in the local system, because there are no options to locally turn on and off the protection, and the settings of categories to block some websites are not provided. AV-Test evaluates antivirus products in a set of three criteria: protection, performance and usability. Sophos received a maximum 6 points for protection in the corporate decision test, and 5 point for performance. In the usability criteria the antivirus received 5.5 points, which means that it issued a small number of false alarms on trusted programs and websites. In total, Sophos gained 16 points out of possible 18 that is very worthwhile result.

In Ukraine “Sophos Enterprise Console”, an antivirus protection program, manufactured by “Sophos Ltd.” And certified by “Sophos Endpoint Security and Control” by “Sophos Ltd.” Production. The totality of the technical requirements determined by the functional security of the profile in accordance to criteria of the technical information.:

3.3. Panzor Cloud Antivirus (USA) [11, 13, 18]. It is an intellectual complex which exists at the same time in the Cloud and on the Endpoint-e – the end-user computing device. This complex provides rapid and effective detection of threats, alerts and responds in real time. In addition to all counted, it supports the protection of computers and networks that operate autonomously but not connected to the Internet. According to the VB information, during 2018 Panzor Cloud Antivirus detected and warned about 94% of known and unknown threats from malicious software without false-positive results.

In Ukraine the Antivirus Software Program “Panzor Cloud Antivirus” version 1 X.X. was certified.

3.4. Developer – **Symantec Corporation** (USA, California), 1982 [11, 12, 19]. According to AV data, Symantec received one Advanced + and four Advanced Awards in the test in 2018.

The Symantec Endpoint Protection 14.XX-XX.XX was certified in Ukraine as an antivirus complex software.

Regarding to the AV data while testing in December 2016 Symantec Endpoint Protection 14.0 achieved the best balance of high level of performance and showed low quantity of false alarms (WPDT – 100%, RTTL – 100%, AVC – 99,4%, FPs – 1,5%).

3.5. Developer – **Laboratory Zillya** (Uktaine), 2009 [11, 20].

Zillya protects user’s device from viruses, spyware, Trojans, rootkits, adware, as well as from unknown threats with the help of the proactive protection. The unique feature of this antivirus is the availability of modern databases of virus signature, which updates every day. It stends to mention that this data does not overload neither the server nor the local PC because the database is optimized and upgraded. Therefore, Zillya work does not affect the speed of the computer, does not lead to hangs, or not slowing down the PC.

Antivirus software "Zillya! Antivirus for Business" version 1.1.xxxx.y is certified in Ukraine. Among its main features need to be mentioned protection of information on the workstations of users and servers of the local network from malicious software (viruses, trojans, spyware and other malicious software) and network attacks. It responds to the requirements of reference documentation (RD) for technical information protection (TIP) in the scope of the functions specified in the document “Antivirus protection software" Zillya! Antivirus for Business”. Technical requirements for the criteria for technical protection of information, the totality of which is determined by the functional profile.:

3.6. Developer – **McAfee** (California, USA) [11, 14, 21].

In Ukraine the McAfee Complete Endpoint Protection – Business (McAfee SERP-C), McAfee Endpoint Threat Defense and Response McAfee version 2.x produced by McAfee Inc. (USA), Software McAfee Complete Endpoint Threat Protection (code – Mcafee CTP), Software McAfee Endpoint Threat Protection (code – McAfee ETP) has been certified.

3.7 Developer – **Bitdefender** (Romania), 2001 [11, 12, 22].

According to AV data, Bitdefender received the “Outstanding Product” award and reached Advanced + level in all seven tests. Additionally, it received the Gold Award for Real-World Test Protection and Silver Awards for False-Positive results in nomination for Malware Protection. The well-designed interface includes real-time protection.

In Ukraine the certification received Bitdefender GravityZone Advanced Business Security software version 6.x (for the Microsoft Hyper-V virtualization platform). It is intended to protect the information resources of information-telecommunication systems of various functional applications from malicious programs, and information attacks of the global telecommunication networks in real-time. Also this antivirus software collects and displays an information about the status of compliance with the security policy adopted by the ITS, providing a centralized managements of security policy in ITS.

3.8. Developer – **Trend Micro** (USA, located in Japan), 1988 [11, 12, 23].

According to AV data, Trend Micro received one award Advanced + and 3 Advanced awards. Reviewers appreciated its distinct design, and easy access to advanced options.

Trend Micro Deep Security software version 10.x. and Trend Micro Enterprise Security for Endpoints Light version OfficeScan XG had received certification in Ukraine.

3.9 Developer – **ROMAD** (Ukraine), 2009 [11, 24].

ROMAD Endpoint Defense is a fully functional new generation antivirus that uses an innovative patented approach to harassing malware. This is a revolutionary approach in cybersecurity. It already works in the markets of Ukraine and Malaysia.

ROMAD Endpoint Defense is the most innovative antivirus of the next generation. It fights families, but not strains. The number of strains now does not matter. ROMAD catches and eradicate prior strains, current strains, and future strains. It gained the reputation in B2B and has received a number of prestigious awards. This antivirus is distributed absolutely for free. End users pay only for successfully repelled attacks.

“ROMAD Endpoint Defense” version 1.x.yyyy for Windows with centralized protection management system is certified in Ukraine as a software product for protection against harmful software.

3.10 Developer **ESET** (Slovakia), 1987 [11, 12, 14].

According to AV data for 2018, ESET received golden award for a false test, silver – for the performance test, four Advanced + and two Advanced awards. The reviewers provide a clear and easy layout of the graphical interface and ease of use.

In Ukraine are certified:

1) Antivirus Protection Software ESET Mail Security for IBM LotusDomino version 4.0.X;

2) ESET Endpoint Antivirus for protecting systems together with ESET Endpoint Antivirus for Windows 6.x with ESET Remote Administrator’s centralized protection system for corporate networks version 6.x;

3) ESET Mail Security Antivirus Software for Microsoft Exchange version 6.x;

4) Antivirus Software for information security ESET Endpoint Protection Advanced together with ESET Endpoint Security for Windows 6.x with centralized antivirus protection managing system for corporate networks ESET Remote Administrator version 6.x;

5) ESET File Security for Microsoft Windows Server version 6.X

6) ESET File Security for Linux/BSD/Solaris version 4.X;

7) ESET Endpoint Antivirus Software for information security as a part of ESET Endpoint Security for Windows version 6.x with centralized antivirus corporate security management networks ESET Remote Administrator version 6.x;

8) ESET Antivirus Software File Security for Linux/BSD/Solaris version 4.X with centralized antivirus corporate security management networks ESET Remote Administrator version 6.x;

9) ESET Mail Security for Linux/BSD/Solaris version 4.X (EMSL);

10) Software Antivirus for information security ESET File Security for Microsoft Windows Server version 6.x with networks ESET Remote Administrator version 6.x;

11) Software Antivirus ESET Gateway Security for Linux/BSD/Solaris version 4.X (EGS);

12) ESET Endpoint Security Antivirus Software for Android together with ESET Endpoint Security for Android version 2.X with ESET Remote Administrator’s centralized antivirus protection system version 6.x;

13) ESET Secure Business Antivirus Protection Software together with ESET Endpoint Security for Windows 6.x with centralized antivirus corporate security management networks ESET Remote Administrator version 6.x;

14) ESET File Security for Microsoft Windows Server version 6.X;

15) ESET File Security for Linux / BSD / Solaris version 4.X;

16) ESET Mail Security for Linux / BSD / Solaris version 4. X, ESET Mail Security for Microsoft Exchange Server version 6.X;

17) ESET Mail Security for IBM Lotus Domino version 4.X;

18) ESET Endpoint Security for Android version 2.X.

Below there are the characteristics of some free antivirus software (Table 1).

Table 1

Analysis of the characteristics of antivirus software products

	Avast Free Antivirus	Sophos Home	Symantec Endpoint Protection	Zillya	McAfee Internet Security	Bitdefender Total Security	Trend Micro Antivirus+ Security	ROMAD Endpoint Defense
Antivirus and antispyware	✓	✓		✓	✓	✓	✓	✓
Antifishing	✓	✓	✓	✓	✓	✓	✓	✓

Antirootkit	✓	✓	✓	✓	✓	✓	✓	✓
Protection against exploits	✓	✓	✓	✓	✓	✓	✓	✓
Intrusion Prevention System (HIPS)	✓	✓	✓	✓	✓	✓	✓	✓
SOHO Protection	✓	✓	✓	✓	✓	✓	✓	✓
Real-time protection	✓	✓	✓	✓	✓	✓	✓	✓
Parental control	✓	✓	✓	✓	✓	✓	-	-
Antispam	✓	✓	✓	✓	✓	✓	✓	✓
Protection against network attacks	✓	✓	✓	✓	✓	✓	✓	✓
Anti-thief	✓	✓	✓	✓	✓	✓	✓	✓
Password managment	✓	-	-	-	✓	✓	-	-
Personal Firewall	✓	✓	✓	✓	✓	✓	✓	✓

It should be noted that in 2014, the National Security Agency of the USA reported that it does not recommend to use Russian antivirus programs: Kaspersky Antivirus, Doctor Web, NOD32.

4. CONCLUSIONS AND PERSPECTIVES FOR FURTHER STUDIES

The results of the study provide an opportunity to evaluate the provision of information security using antivirus programs that are certified in Ukraine. They can be used by information security lecturers when preparing for lectures and practical classes, and these materials can be applied when students conduct laboratory work in a virtual laboratory [26] in order to develop practical skills and knowledge in the field of information security.

REFERENCES

[1] Steve Morgan, Editor-in-Chief Cybersecurity Ventures. 2017 Cybercrime Report. Herjavec group. Режим доступу: https://cybersecurityventures.com/2015-wp/wpcontent/uploads/2017/10/2017-Cybercrime-Report.pdf.

[2] Cisko report on cybersecurity 2019 – Access mode: https://www.cisco.com/c/uk_ua/products/security/security-reports.html#~stickynav=2

[3] Svchenko A.S., Penkova I.V. An analysis of antivirus software application for information secutiry http://dspace.nbuv.gov.ua/bitstream/handle/123456789/93924/31-Ivchenko.pdf?sequence=1

[4] Smirnov S.A. Antivirus data protection method which uses cloud computing technologies. The dissertation for the degree of candidate of technical sciences. Access mode: http://www.dut.edu.ua/uploads/p_1539_60443732.pdf

[5] Nizovtsev Yu. The usage of antivirus software in forensic expertise against malicious software means / Yu. Nizovtsev, O. Yakovlev // Scientific journal of the National Academy of Public Prosecutor of Ukraine. – 2017. – № 4(16). – P. 161–169. Access mode: http://www.chasopysnapu.gp.gov.ua/chasopys/ua/pdf/4-2017/nizovcev.pdf

[6] Rudnichenko A.K. Kolesnikova D.S., Vereschahina E.A. Protection against malicious software that look as a complex of legitimate software products // Internet journal «Naukovedenie», №9(5), 2017 . Access mode: https://naukovedenie.ru/PDF/72TVN517.pdf .

[7] S.G. Semenov. Development of computer virus detection system, based on the neural network APT -1 / S. Semenov, S. Havrilenko, S. Hloba, O. Babenko // Systems of information processing. – 2015. - № 10(135). – p. 126 – 129.

[8] AV-TEST - The Independent IT-Security Institute, 2019. Access mode: https://www.av-test.org/en/statistics/malware/.

[9] The order of updating an antivirus software that has a positive conclusion on the results of state expertise in the field of technical protection of information. Access mode: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?art_id=50825&cat_id=38835

[10] Buryachok V.L. Informational and cyberspaces: security issues, methods and means of struggle. / V.L.Buryacjok, G.M.Gulak, V.L. Tolubko. – K. : PLC “SIC GROUP Ukraine”, 2015. – p.449

[11] The list of АВПЗ, which receive positive expert opinion. Access mode: http://cazi.gov.ua/p.php

[12] Summary Report 2018 AV-Comparatives. Access mode: https://www.av-comparatives.org/tests/summary-report-2018/

[13] VB Testing Virus Bulletin's testing and certification services. Access mode: https://www.virusbulletin.com/testing/

[14] Antivirus rating 2019 – Let’s choose the best antivirus. Access mode: http://softcatalog.info/ru/obzor/reyting-antivirusov

[15] Avast Free Antivirus. Access mode: https://www.avast.ua/ru-ua/free-antivirus-download

[16] Avast Free Antivirus. Access mode: https://avast.ru.softonic.com/

[17] Sophos Home. Access mode: https://www.comss.ru/page.php?id=2879

[18] Panzor CloudAntivirus Always Protected. Access mode: https://panzor.com/

[19] Symantec Endpoint Protection 14. Access mode: https://www.anti-malware.ru/reviews/Symantec_Endpoint_Protection_14

[20] Antivirus Zillya. Access mode: https://zillya.ua/zillya-total-security?product=zts3&term=12&count=1

[21] McAfee Internet Security. Access mode: https://www.mcafee.com/consumer/ru-ru/store/m0/catalog/mis_516/mcafee-internet-security.html

[22] Bitdefender Total Security. Access mode: https://bitdefender.com.ua/product/bitdefender-total-security/

[23] Antivirus plus Security. Access mode: https://www.trendmicro.com/en_us/forHome/products/antivirus-plus.html

[24] ROMAD Cyber Systems. Access mode: https://romad-systems.com/ua/

[25] Decree of the President of Ukraine No.133/2017 On decision of the National Security and Defense Council of Ukraine dated April 28, 2017 “On the Application of Personal Special Economic and Other Restrictive Measures (Sanctions)”. Access mode: https://www.president.gov.ua/documents/1332017-21850

[26] V. Buriachok, S. Shevchenko, and P. Skladannyi, “Virtual Laboratory for Modeling of Processes in Informational and Cyber Securities as a form of Forming Practical Skills of Students”, Cybersecurity: Education, Science, Technique, vol. 2, no. 2, pp. 98-104. https://doi.org/10.28925/2663-4023.2018.2.98104

Шевченко Світлана Миколаївна
кандидат педагогічних наук, доцент, доцент кафедри комп'ютерних наук і математики
Київський університет ім. Бориса Грінченка, м. Київ, Україна
OrcID 0000-0002-9736-8623
s.shevchenko@kubg.edu.ua

Складаний Павло Миколайович
старший викладач кафедри інформаційної та кібернетичної безпеки
Київський університет імені Бориса Грінченка, Київ, Україна
OrcID 0000-0002-7775-6039
p.skladannyi@kubg.edu.ua

Марценюк Максим Станіславович
студент кафедри інформаційної та кібернетичної безпеки
Київський університет імені Бориса Грінченка, Київ, Україна
OrcID 0000-0002-6662-7610
msmartseniuk.fitu18@kubg.edu.ua

АНАЛІЗ ТА ДОСЛІДЖЕННЯ ХАРАКТЕРИСТИК АНТИВІРУСНОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ, СТАНДАРТИЗОВАНОГО В УКРАЇНІ

Анотація. Стаття присвячена проблемі забезпечення захисту інформації, а саме дослідженню характеристик антивірусних програм, які стандартизовані в Україні. У дослідженні були використані статистичні методи аналізу характеристик антивірусного програмного забезпечення та порівняльні методи зіставлення різних видів таких програм. Спираючись на дослідження у науковій літературі, були проаналізовані основні загрози інформаційної безпеки у сфері інформаційних технологій. Зроблено наголос на те, що антивірусне програмне забезпечення є найбільш ефективним засобом захисту проти шкідливого програмного забезпечення (malware). Описані основні методи роботи антивірусного програмного забезпечення: сигнатурний та евристичний. Визначено перелік антивірусних програм, які стандартизовані в Україні. Дослідження ґрунтувалося на кількісних та якісних результатах, одержаних при тестуванні незалежною тестовою лабораторією AV-Comparatives (Австрія), незалежною лабораторією Virus Bulletin (VB) з тестування та сертифікації в області безпеки, Центром антивірусного захисту інформації Держспецзв'язку України. Здійснено порівняльний аналіз основних характеристик антивірусних програм, а саме: антивірус та антишпигун; антифішинг; антикруткіт; захист від експлойтів; система запобігання вторгненням; захист у режимі реального часу; батьківський контроль; персональний брандмауер; антиспам; захист від мережевих атак; захист домашньої мережі; антикрадій; управління паролями.

Ключові слова: антивірусне програмне забезпечення; захист інформації; характеристики антивірусних програм; шкідливе програмне забезпечення (malware).

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] Steve Morgan, Editor-in-Chief Cybersecurity Ventures. 2017 Cybercrime Report. Herjavec group. Режим доступу: https://cybersecurityventures.com/2015-wp/wpcontent/uploads/2017/10/2017-Cybercrime-Report.pdf.

[2] Звіт Cisko із кібербезпеки за 2018 рік. – Режим доступу https://www.cisco.com/c/uk_ua/products/security/security-reports.html#~stickynav=2

[3] Ивченко А.С., Пенькова И. В. Анализ применения антивирусного программного обеспечения для информационной безопасности. Режим доступу: http://dspace.nbuv.gov.ua/bitstream/handle/123456789/93924/31-Ivchenko.pdf?sequence=1

[4] Смирнов С.А. Метод антивирусной защиты данных с использованием облачных вычислительных технологий. Диссертация на соискание ученой степени кандидата технических наук. Режим доступу: http://www.dut.edu.ua/uploads/p_1539_60443732.pdf .

[5] Ю. Нізовцев та О. Яковлєв, «Використання антивірусних програм при проведенні судових експертиз шкідливих програмних засобів», Науковий часопис Національної академії прокуратури України, №4(16), сс. 161-169, 2017. Режим доступу: http://www.chasopysnapu.gp.gov.ua/chasopys/ua/pdf/4-2017/nizovcev.pdf.

[6] А. Рудниченко, Д. Колесникова та Е. Верещагина, «Защита от вредоносного программного обеспечения, представляющего собой комплекс легитимных программных продуктов», Интернет-журнал «НАУКОВЕДЕНИЕ», №9(5), 2017. Режим доступу: https://naukovedenie.ru/PDF/72TVN517.pdf .

[7] Розробка системи виявлення комп’ютерних вірусів на основі нейронної мережі АРТ-1 / С.Г. Семенов, С.Ю. Гавриленко, С.М. Глоба, О.С. Бабенко // Системи обробки інформації. – 2015. – № 10(135). – С. 126-129.

[8] AV-TEST - The Independent IT-Security Institute, 2019. Режим доступу: https://www.av-test.org/en/statistics/malware/ .

[9] Порядок оновлення антивірусних програмних засобів, які мають позитивний висновок за результатами державної експертизи в сфері технічного захисту інформації. Режим доступу: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?art_id=50825&cat_id=38835

[10] В. Бурячок, Г. Гулак та В. Толубко, Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби. ТОВ «СІК ГРУП УКРАЇНА», 2015, с. 449.

[11] Перелік АВПЗ, які мають позитивний експертний висновок . Режим доступу:http://cazi.gov.ua/p.php

[12] Summary Report 2018 AV-Comparatives. Режим доступу: https://www.av-comparatives.org/tests/summary-report-2018/.

[13] VB Testing Virus Bulletin's testing and certification services. Режим доступу: https://www.virusbulletin.com/testing/

[14] Рейтинг антивирусов 2019 – Выбираем лучший антивирус. Режим доступу: http://softcatalog.info/ru/obzor/reyting-antivirusov

[15] Avast Free Antivirus. Режим доступу: https://www.avast.ua/free-antivirus-download

[16] Avast Free Antivirus. Режим доступу: https://avast.ru.softonic.com/

[17] Обзор Sophos Home. Режим доступу: https://www.comss.ru/page.php?id=2879

[18] Panzor CloudAntivirus Always Protected. Режим доступу: https://panzor.com/

[19] Обзор Symantec Endpoint Protection 14. Режим доступу: https://www.anti-malware.ru/reviews/Symantec_Endpoint_Protection_14

[20] Антивірус Zillya. Режим доступу:https://zillya.ua/zillya-total-security?product=zts3&term=12&count=1

[21] McAfee Internet Security . Режим доступу: https://www.mcafee.com/consumer/ru-ru/store/m0/catalog/mis_516/mcafee-internet-security.html

[22] Bitdefender Total Security. Режим доступу: https://bitdefender.com.ua/product/bitdefender-total-security/

[23] Antivirus plus Security. Режим доступу: https://www.trendmicro.com/en_us/forHome/products/antivirus-plus.html

[24] ROMAD Cyber Systems. Режим доступу: https://romad-systems.com/ua/

[25] Указ Президента України № 133/2017 Про рішення Ради національної безпеки і оборони України від 28 квітня 2017 року «Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій)». Режим доступу: https://www.president.gov.ua/documents/1332017-21850

[26] В. Бурячок, С. Шевченко, та П. Складанний, «ВІРТУАЛЬНА ЛАБОРАТОРІЯ ДЛЯ МОДЕЛЮВАННЯ ПРОЦЕСІВ В ІНФОРМАЦІЙНІЙ ТА КІБЕРБЕЗПЕЦІ ЯК ЗАСІБ ФОРМУВАННЯ ПРАКТИЧНИХ НАВИЧОК СТУДЕНТІВ», *Кібербезпека: освіта, наука, техніка*, том 2, номер 2, стор 98-104. https://doi.org/10.28925/2663-4023.2018.2.98104