Czech University of Life Sciences Prague

Faculty of Economics and Management

Department of Information Technology

Bachelor Thesis

Information security

Ivan Devyatkin

CZECH UNIVERSITY OF LIFE SCIENCES PRAGUE

Faculty of Economics and Management

BACHELOR THESIS ASSIGNMENT

Ivan Devyatkin

Systems Engineering and Informatics
Informatics

Thesis title

Information Security

Objectives of thesis

The main goal of this bachelor thesis is to identify the most suitable products for protecting personal computers from malicious programs. Partial goals to achieve this result are as follows:
- conduct review of available literary and online sources regarding antivirus software, forms of protection and types of attacks
- analyze existing antivirus software based on selected criteria
- compare different solutions and select optimal variant for protection of personal computers

Methodology

The methodology of the practical part of the thesis will be based on experimental testing and multi-criteria evaluation of variants. The best product will be determined by empirical comparison of available solutions. Conclusions will be formulated based on the conjunction of obtained theoretical knowledge and the practical results.

The proposed extent of the thesis

35-50

Keywords

Information security, antivirus software, malware, cybercrime

---

Recommended information sources

Blokdyk, Gerardus. Antivirus software: A Complete Guide. s.l. : CreateSpace Independent Publishing Platform, 2018. ISBN-13: 978-1718608214

Joshua Saxe, Hillary Sanders. Malware Data Science: Attack Detection and Attribution. s.l. : No Starch Press , 2018. ISBN: 1593278594

Joxean Koret, Elias Bachaalany. The Antivirus Hacker's Handbook. Indianapolis : John Wiley and Sons, Inc., 2015. ISBN-13: 978-1119028758

Expected date of thesis defence

2020/21 SS – FEM

The Bachelor Thesis Supervisor

Ing. Jan Pavlík

Supervising department

Department of Information Technologies

Electronic approval: 20. 7. 2020

Ing. Jiří Vaněk, Ph.D.

Head of department

Electronic approval: 19. 10. 2020

Ing. Martin Pelikán, Ph.D.

Dean

Prague on 28. 02. 2021

Declaration

I declare that I have worked on my bachelor thesis titled "Information security" by myself and I have used only the sources mentioned at the end of the thesis. As the author of the bachelor thesis, I declare that the thesis does not break any copyrights.

In Prague on 15.03.2021 _____

Acknowledgement

I would like to thank my supervisor ing. Jan Pavlík for the joint work done. I would also like to thank my friends for their support in the daily struggle for knowledge. This path would be much more difficult without you.

Information security

Abstract

This bachelor thesis was written with the goal of identifying the best security software for a personal computer. The thesis consists of two parts: a theoretical part and a practical part.

Theoretical part includes a description of computer viruses, their types and classification. In addition to information about malicious programs, the theoretical part contains data about antiviruses (types of security programs, history of antivirus development, types of testing of antivirus programs).

Practical part includes testing itself according to the selected criteria, with the help of which the best antivirus will be determined.

Keywords: Information security, antivirus, virus, malware, test, protection, threat, methodology of testing, experimental testing

Informační bezpečnost

Abstrakt

Tato bakalářská práce byla napsána s cílem identifikovat nejlepší bezpečnostní software pro osobní počítač. Práce se skládá ze dvou částí: teoretické a praktické.

Teoretická část obsahuje popis počítačových virů, jejich typů a klasifikace. Kromě informací o škodlivých programech obsahuje teoretická část také údaje o antivirech (typy bezpečnostních programů, historie vývoje antivirů, typy testování antivirových programů).

Praktická část zahrnuje samotné testování podle vybraných kritérií, pomocí kterého bude určen nejlepší antivirus.

Klíčová slova: Informační bezpečnost, antivirus, virus, malware, test, ochrana, hrozba, metodika testování, experimentální testování

Table of content

List of pictures

List of tables

1 Introduction

Information security or cybersecurity is not rare definitions nowadays. Defending of personal data in the world wide web as much important as in the "offline" world or maybe it is more important.

Most of social and professional life in 21st century is online. Especially now, when all business centers, offices and others working places are closed because of known cause, personal or corporate electronic devices have become the main tool for connection with others.

Malicious computer programs can be cause of leaks of information, blocking work of operation system or even "steal" computer power. Kaspersky web-site confirms previous statement that these programs (malicious computer programs) are installed without the consent of users and can cause a number of unpleasant effects, including crippling computer performance, mining your system for personally identifiable information (PII) and sensitive data, erasing or encrypting data or even hijacking device operations or computer-controlled hardware. (1)

That is why the goal of theoretical part of bachelor thesis is striving to provide useful information about main types malware programs and how to defend personal computers from them using antivirus software and how to choose this protection wisely. As Clifford wrote in his book that the hacker didn't succeed through sophistication. Rather he poked at obvious places, trying to enter through unlock doors. Persistence, not wizardry, let him through.. Properly chosen antivirus will help to reduce chances to enter through unlock doors. (2)

2 Objectives and Methodology

2.1 Objectives

The main goal of this bachelor thesis is to identify the most suitable products for protecting personal computers from malicious programs. Partial goals to achieve this result are as follows:

- conduct review of available literary and online sources regarding antivirus software, forms of protection and types of attacks
- analyze existing antivirus software based on selected criteria
- compare different solutions and select optimal variant for protection of personal computers

2.2 Methodology

The methodology of the practical part of the thesis will be based on experimental testing and multi-criteria evaluation of variants. The best product will be determined by empirical comparison of available solutions. Conclusions will be formulated based on the conjunction of obtained theoretical knowledge and the practical results.

3 Literature Review

3.1 Malicious programs

Malicious software is different and before discussing antiviruses, it is crucial to know what computer viruses exist to find out how to defend personal computer and personal data.

What are computer viruses? According to definition on www.malwarebytes.com website: a computer virus is malware attached to another program (such as a document), which can replicate and spread after an initial execution on a target system where human interaction is required. Many viruses are harmful and can destroy data, slow down system resources, and log keystrokes. (3)

This definition clearly mentioned a lot of types of viruses. Each of these programs could be dangerous for hardware and software in case of lack of information about them. In this part will be introduced the main types of malicious programs. Such as:

- Viruses
- Worms
- Adware
- Spyware
- Ransonware
- Bots
- Rootkits
- Trojans
- Bugs

These malicious programs are the most common software to get access to users' data. That is why they were chosen. (4)

3.1.1 Viruses

Computer viruses get their name for their ability to "infect" many files on a computer. They spread to other machines as well when infected files are sent by email or transferred by users on physical media such as USB sticks or (formerly) floppy disks. According to the National Institute of Standards and Technology (NIST), the first computer virus called "Brain" was written in 1986 by two brothers to punish pirates who steal software from the company. The virus infected the boot sector of floppy disks and was transmitted to other computers through the copied infected floppy disks.

Classification of computer viruses

Computer viruses can be systematized by the platforms they target and for which operating systems they are written (Microsoft Windows, Linux, etc.), as well as by the objects of infection (boot, file, script), by the technologies used, by the programming languages.

Viruses can also be classified according to their mode of action:

Rewriters. Such infections write themselves instead of the original program code without changing the file name. As a result, the infected application simply stops working and the malware is executed instead.

Parasitic. These viruses inscribe their code anywhere in the executable file. The infected program works in whole or in part.

Companion viruses. After self-copying, they rename or move the original file. As a result, the legitimate program works, but only after the virus code has been executed.

Link viruses. Such malicious code changes the location of the software to its own. Thus, it forces the operating system to run it without any changes to the code of other applications.

Destructive viruses. This can include malicious objects that simply damage the original code of the program or its components to disable them.

Object of influence

Any computer can be a target, but most viruses target the Windows platform. New computer viruses capable of replicating and infecting executable files are very rare today. The peak of their distribution came at the end of the 90s of the XX century. With the spread of computer networks and the Internet, file viruses began to rapidly lose their relevance, as simpler ways of spreading malicious programs appeared.

Source of threat. There are several main ways of infecting computer systems with file viruses.

Removable media. These can be pre-prepared floppy disks, optical disks, USB sticks. Floppy disks are not relevant today, but mobile phones and smartphones, digital cameras, camcorders and players have joined the ranks of carriers of dangerous information.

Through local networks. Once on a file server, a virus spreads quickly to other computers. (5)

3.1.2 Worms

Unlike viruses, worms do not require human intervention to spread they infect one computer and then spread through computer networks to other machines without the participation of their owners. By exploiting network vulnerabilities, such as flaws in email programs, worms can send thousands of copies of themselves and infect new systems, and then the process starts again. In addition to the fact that many worms simply "eat" system resources, thereby reducing the performance of the computer, most of them now contain malicious "components" designed to steal or delete files.

Malicious software from the subclass of viruses and worms includes:

- Email-Worm
- IM-Worm
- IRC-Worm
- Net-Worm
- P2P-Worm
- Virus
- Computer worms

Most of the known computer worms spread in the following ways:

- as a file sent as an attachment in an email
- as a link to the Internet - or FTP resource
- as a link sent via ICQ or IR message
- through peer-to-peer communication networks P2P

some worms spread as network packets. They penetrate directly into computer memory, then the worm's code is activated.

Computer worms can exploit network configuration errors (for example, to copy themselves to a fully accessible disk) or vulnerabilities in the operating system and applications. Many worms spread copies of themselves across the network in several ways. (6)

Viruses

Viruses can be classified according to the way in which they infect a computer:

- File viruses

- boot sector viruses
- Macroviruses
- Virus scripts

3.1.3 Adware

One of the most common types of malware is adware. The programs automatically deliver advertisements to host computers. Adware flavors include pop-up advertisements on web pages and advertisements included in "free" software. Some adware programs are relatively harmless, others use tracking tools to collect information about your location or browsing history and display targeted ads on your computer screen. BetaNews reported the discovery of a new type of adware that could disable antivirus protection. Since Adware is installed with the user's consent, such programs cannot be called malicious: they are usually identified as “potentially unwanted software”. (7)

Adware classification

Adware classification can be divided into adware programs according to the method of implementation: in some cases, they are executed as an independent application that starts from the start of the system, in others, they are a module that is embedded in existing processes. For example, the target of such an implementation could be an Internet browser.

Online adware is used in programs that require an internet connection to run. The download of banner ads comes from an external source and resembles advertisements on websites. You can also come across samples that do not require connection: a pre-prepared set of banners is stored on the computer disk along with the rest of the software.

Advertising programs are distributed in legal and illegal ways. In the first case, the developer receives an additional component from the advertising network, which is built in at the stage of creating the application, and in the second case, attackers distribute such modules through illegal channels for the purpose of profit.

Source of threats There are several ways adware appears on your computer.

The first option is along with free software. Showing ads generates revenue for developers, which is spent on further improving their application. This is a completely legitimate scenario, and the user is usually warned of the presence of advertisements.

The second way is through infected sites. After going to such a site, the program is installed without warning. To inject it, hackers use browser vulnerabilities. This type of adware is called Browser Hijackers.

Also, the ad module can be downloaded and installed by a malicious agent already present in the system, for example, a Trojan downloader.

You can get rid of annoying ads using an antivirus. If the program is installed without your permission, then this is the main reason to believe that it poses a danger to your data. It is recommended to completely remove such an object.

Some freeware programs stop showing advertisements after purchasing a license. However, if the presence of adware components in them is since their code has been hacked, then purchasing the paid version will not help. Ads will continue to run, and the utility may not work correctly.

Some programmers mask files of unwanted parts of their applications. As a result, the antivirus does not recognize them as a threat, considering it an integral part of the program, without which correct operation is impossible. For such cases, there are special tools that remove ads without disrupting the operation of the entire software. (8)

3.1.4 Spyware

Spyware does what its name suggests - it spy on your computer. It collects information (for example, logs keystrokes on your computer's keyboard, tracks which sites you visit, and even intercepts your registration data), which is then sent to third parties, usually cybercriminals. It can also change certain security settings on your computer or interfere with network connections. According to TechEye, new types of spyware allow attackers to monitor user behavior (of course, without their consent) on different devices.

Spyware classification

Trackers transmit to the attacker data about the location of the device, websites opened, documents, contact lists, travel route, most frequently visited places, etc. Trackers are divided into two types: hardware and software. Hardware trackers look like a miniature device, like a keychain. Most of them simply transmit data about the current position of the object, but some options have broader functionality. They can be legal - they are used by motorists to obtain information about the current position of their car, they can be used to find out the location of valuable things, etc. Software trackers are used to collect any data about user activity on the device. They can also be legal: they are used by organizations wishing to monitor employees during working hours, or by parents who are worried about their child. Both categories of trackers can be used by cybercriminals to unauthorized collection of information about a victim's movement. A hardware tracker can be inconspicuously

embedded in one of the components of a computer, while a software tracker can be installed under the guise of some legal program or together with it. Legal trackers include all kinds of toolbars for browsers or entire Internet browsers produced by search engines and major Internet portals such as Yahoo, Yandex or Mail.ru. Such products, with the user's permission or ignorance, collect comprehensive information about Internet surfing, which is used in the development of services and targeting advertising.

Keyloggers are special programs or devices that record keystrokes on the device's keyboard. Like trackers, keyloggers are divided into two types: hardware and software. Software keyloggers run as applications, so each operating system has its own set of such tools. Many of them can read not only regular keystrokes, but also service keys, such as Alt or Ctrl, thereby fixing the output of commands through key combinations. Several keyloggers send collected data to scammers and other attackers. Hardware keyloggers are small devices that plug into your computer. Some of them can exploit the BadUSB vulnerability. Unlike software keyloggers, hardware keyloggers do not affect the hard drive in any way: they save all data to the built-in memory or to an SD card. (9)

3.1.5 Ransomware

Ransomware infects your computer, then encrypts sensitive data, such as personal documents or photos, and demands a ransom to decrypt them. If you refuse to pay, the data is deleted. Certain types of ransomware can completely block access to your computer. They can present their actions as the work of law enforcement agencies and accuse you of any illegal actions. In April 2014, the FBI's Internet Fraud Complaint Center was contacted by users who reported financial losses totaling $ 18,000,000 as a result of the CryptoWall ransomware virus. (10)

Ransomware classification

Ransomware is divided into three types based on how they work: Encrypting files on the system. Obstruction of work with the PC. Interfering with browsers.
In the first case, the program subjects the victim's files to cryptographic transformation and requires payment for providing a decryption key or a special decryptor utility.

In the second case, the program makes working with the victim's computer completely or partially impossible. A classic example of such a ransomware is WinLocker. This type is the most common due to the ease of writing such programs.

Malicious objects of the third type interfere with the operation of Internet browsers by blocking the main window with an advertising banner or by intimidating users that they have allegedly committed illegal actions. One way or another, they are extorting money for unlocking.

The ransomware spreads in the same way as any other instance of malicious code: using spam mailing, physical contact of an attacker with the victim's computer, downloading infected files, etc.

Target of ransomware viruses

Ransomware doesn't always target a personal computer. Since the cybercriminal's job is to extract financial gain, it makes sense for him to attack small and medium-sized companies: they are more solvent than a home user, and an encrypted accounting database is a much more powerful incentive to pay ransom than an archive of personal photos. For example, in 2016, 42% of such companies were attacked by ransomware, of which 32% paid the ransom, and 20% never got access to their data. The ransomware was first recorded in May 2005. Since then, their number and variety have greatly increased. Gradually, the ransomware became smarter: they began to demand untracked transactions in bitcoins, encrypt data. Some modern ransomware is even equipped with tech support. The most famous families are Cryzip, Krotten, Archiveus. Experts from many antivirus companies have named ransomware ransomware as the main topic of 2016.

Source of threat

Ransomware is very widespread due to the simplicity of its creation. There are many sources of threat: infected sites, files, vulnerabilities in email clients, flaws in the OS (for example, WinLocker uses only standard Windows functions). There is an opinion that most of the creators of ransomware Trojans are from Russia, since local authorities do not fight this type of crime in any way. Some ransomware “do not keep their promises” and even after payment they do not unlock the computer or decrypt files. (11)

3.1.6 Bots

Bots are programs designed to automatically perform certain operations. They can be used for legitimate purposes, but the attackers have adapted them for their malicious purposes. Once inside a computer, bots can force it to execute certain commands without approval or even without the user's knowledge. Hackers can also try to infect multiple computers with the

same bot to create a botnet that can then be used to remotely control compromised machines - steal sensitive data, spy on the victim, automatically spread spam, or launch devastating DDoS attacks on computer networks. (12)

3.1.7 Rootkits

Rootkits allow a third party to remotely access and control a computer. These programs are used by IT professionals to remotely troubleshoot network problems. But in the hands of cybercriminals, they turn into a fraudulent tool: once they get into your computer, rootkits provide cybercriminals with an opportunity to take control of it and steal your data or install other malware. Rootkits are able to efficiently mask their presence in the system in order to remain unnoticed for as long as possible. Detecting such malicious code requires manual monitoring of unusual behavior, as well as regular software and operating system adjustments to eliminate potential infection routes.

Rootkit classification

By the type of privilege, rootkits are divided into two types: user (performs actions on behalf of the user account) and operating at the kernel level. The principle of operation of rootkits can also be divided into two categories: modifying algorithms of system functions and modifying system data structures.

On Windows operating systems, rootkits can work in the following ways:

1. Capturing call tables Such a rootkit is capable of acting both at the user level and at the kernel level. By modifying the table, it redirects system function calls to the addresses it needs - for example, to those where the Trojan's functions are located. As a result, the intercepted procedure can bypass the antivirus (by blocking calls from it) or replace the original function. There is reason to believe that this type of rootkit is the most sophisticated. Its capabilities are wider than that of the second type, described below. This is due to the fact that call table hijacking rootkits can operate both at the kernel and user levels.

2. Modification of the function code With this type of rootkit operation, the first few bytes of the called function are replaced with malicious code. The implementation of this approach has a nuance: for each call of an intercepted function, you must first restore its machine code to the state in which it was before the call, in order to intercept it again later.

The interceptor works according to the following algorithm:

1. Performs actions as intended by the attacker.
2. Recovers the first bytes of the intercepted function.
3. Parses the output of the function.
4. Returns control of the function to the system.

Also, to intercept the function, you can replace its first bytes with the jmp operation, which transfers control to the rootkit. However, such an operation is easy to expose if you check the first bytes of the called functions for its presence, so most cybercriminals "overwrite" several bytes before the jmp operation with meaningless operations like mov a, b.
For UNIX-like operating systems, rootkits can be implemented in the following ways:
1. Replacing system utilities.
2. As a kernel module. With VFS patching.
3. Interception of tables of system calls. By changing the physical memory of the kernel. (13)

3.1.8 Trojans

Better known as Trojans, these programs are disguised as legitimate files or software. Once downloaded and installed, they make changes to the system and carry out malicious activities without the knowledge or consent of the victim.

Trojans are classified according to the type of actions they perform on the computer.

Backdoors. The backdoor Trojan provides cybercriminals with the ability to remotely control infected computers. Such programs allow the author to perform any action on the infected computer, including sending, receiving, opening and deleting files, displaying data, and restarting the computer. Backdoor Trojans are often used to combine a group of victim computers into a botnet or zombie network for criminal use.

Exploits. Programs with data or code that exploit a vulnerability in applications running on a computer.

Rootkits. Programs designed to hide certain objects or actions in the system. Often, their main goal is to prevent the detection of malicious programs to increase the running time of these programs on the infected computer.

Banking Trojans. Banking Trojans (Trojan-Banker) are designed to steal the credentials of online banking systems, electronic payment systems, and credit or debit cards.

DDoS Trojans. These programs are designed to carry out Denial of Service (DoS) attacks against targeted web addresses. In such an attack, a large number of requests are sent from infected computers to the system with a specific address, which can cause its overload and lead to denial of service.

Trojan-Downloader. Trojan-Downloader programs are capable of downloading and installing new versions of malicious programs, including Trojans and adware, on a victim computer.

Trojan-Dropper. These programs are used by hackers to install Trojans and / or viruses or prevent malware from being detected. Not every antivirus program is capable of detecting all components of this type of Trojan.

Trojan-FakeAV. Programs like Trojan-FakeAV mimic the operation of antivirus software. They are designed to extort money from the user in exchange for the promise of detecting and removing threats, even though the threats they report do not really exist.

Gaming Trojans. Programs of this type steal information about the accounts of participants in online games.

IM Trojans. Trojan-IM programs steal logins and passwords for instant messaging programs such as ICQ, MSN Messenger, AOL Instant Messenger, Yahoo Pager, Skype and many others.

Trojan-Ransom. This type of Trojan can alter data on a computer in such a way that the computer stops working normally and the user is unable to use certain data. The attacker promises to restore normal operation of the computer or unblock the data after payment of the requested amount.

SMS Trojans. These programs send text messages from your mobile device to premium premium phone numbers, spending your money.

Spyware. Programs such as Trojan-Spy can covertly monitor computer usage, for example, by monitoring keyboard input, taking screenshots, and retrieving a list of running applications.

Trojan-Mailfinder. Such programs can collect email addresses from your computer. (14)

There are also other types of Trojans:

- Trojan-ArcBomb
- Trojan-Clicker
- Trojan-Notifier

- Trojan-Proxy
- Trojan-PSW

3.1.9 Bugs

Bugs - errors in fragments of program code are not a type of malware, but errors made by a programmer. They can have detrimental effects on your computer, such as stopping, crashing, or slowing performance. At the same time, security bugs are an easy way for attackers to bypass security and infect your machine. Providing more effective security controls on the developer's side helps fix bugs, but it's also important to make regular software adjustments to address specific bugs. (15)

3.2 Antivirus programs

Antivirus program (antivirus) is a specialized program for detecting computer viruses, as well as unwanted programs in general and restoring files infected with such programs, as well as for prevention - preventing infection of files or the operating system with malicious code.

There are many types of antivirus programs and ways how they perform and defend data and personal computers such as:

- Scanners
- Monitors
- Polyphages
- Auditors
- Blockers

Also, varieties of defense can be different: proactive defense or reactive defense. It depends on type of the threat.

This part will provide specific information about antivirus programs and their different types and features.

This knowledge will be so useful in practical part to choose the best product among all.

3.2.1 History of antivirus programs

The first antivirus programs appeared in the winter of 1984 (the first virus for Apple personal computers appeared in 1977, and only in 1981 did viruses that pose any threat

appear) under the names CHK4BOMB and BOMBSQAD. They were written by American programmer Andy Hopkins. CHK4BOMB made it possible to analyze the text of the load module and identify all text messages and "suspicious" code sections. BOMBSQAD intercepted BIOS write and format operations. When a prohibited operation was detected, it could be allowed or denied.

The first antivirus in the modern sense of this term, that is, resident, "protecting" from virus attacks, appeared in 1985. The DRPROTECT program was created by Gee Wong. The development blocked all operations (writing, formatting) performed through the BIOS. If such an operation was detected, the program demanded a system restart.

Until the early 90s, anti-virus programs were, in fact, a set of several dozen signatures (samples of virus code) that were stored in the body of the program. The procedure for searching for these signatures in files was also assumed. And often the developers did not even encrypt these signatures. It turned out that sometimes one antivirus could easily “find a virus” in another. The complication of the situation with viruses led to the complication of programs that were designed to fight them. As is usually the case, very soon the initiative to develop and subsequently sell antivirus programs passed to large companies, which, of course, consist of more than one enthusiastic programmer. We are proud to note that programmers from Russia have played a leading role in the development of this industry.

In 1992, the MtE program appeared - a generator of polymorphic (constantly changing) code, which could be used not only by an experienced, but also by any novice programmer. Polymorphic viruses began to appear every day, and all sorts of additional methods of struggle, such as the complication of algorithmic code verification languages, stopped working. The only thing that saved the situation was the appearance of a code emulator. The system "removed" the encrypted part of the polymorphic virus and reached the permanent body of the virus. The first antivirus program with an emulator was the AVP of Eugene Kaspersky.

In addition to the code emulator, which allowed antiviruses to adapt to the rapidly growing "virus industry", around the same time, such protection systems as cryptanalysis, statistical analysis, heuristic analyser, and behavioural blocker appeared. We will not describe what their essence is, we will only note that based on their principles, which were set already more than 15 years ago, antiviruses for the most part "leave" until now.

With the advent of Windows with its inherent multitasking and an extensive system of complex programs, new requirements for antivirus vendors have emerged. Among them - the need to check files on the fly (at the time of access to them) and good work with programs

such as Microsoft Office. The number of antivirus developers then dropped sharply due to the more stringent requirements imposed on them over time. True, their profits have grown significantly. Anti-virus software developers responded to the widespread use of the Internet and the development of malicious (spyware) programs disguising themselves as ordinary ones following it by introducing “gateway, perimeter protection” - firewalls. At the moment, the fight against viruses continues. There are now about 60 companies developing antivirus software around the world.

But the situation may change - the antivirus market, the best samples of which have always been paid, is exploding Microsoft with its completely free Microsoft Security Essentials, developed by the most experienced specialists on the basis of developments used in business security products - Forefront. The quality and level of protection of Microsoft Security Essentials is not inferior to its paid counterparts. Following the introduction of the Net into every home, antiviruses also become readily available. However, on one condition: the Windows version must be licensed. (16)

3.2.2 Types of antivirus programs

Scanners. After starting, they scan the file system and RAM (random access memory) of the PC and neutralize the found viruses.

Monitors. They monitor the processes running on the computer in real time.

Polyphages. The most popular and effective anti-virus programs are polyphage anti-virus programs (for example, Kaspersky Anti-Virus, Dr.Web). The principle of operation of polyphages is based on scanning files, boot sectors of disks and RAM and searching them for known and new (unknown to the polyphage) viruses.

Auditors. The principle of operation of auditors (for example, ADinf) is based on calculating checksums for files present on the disk. These checksums are then saved in the anti-virus database, as well as some other information: file lengths, dates of their last modification, etc. The disadvantage of auditors is that they cannot detect a virus in new files (on floppy disks, when unpacking files from an archive, in email) because their databases lack information about these files.

Blockers. Anti-virus blockers are programs that intercept "virus-dangerous" situations and inform the user about it. Such situations include, for example, writing to the boot sector of a disk. This recording occurs when a new operating system is installed on the computer or when infected with a boot virus. The advantages of blockers include their ability to detect and stop a virus at the earliest stage of its reproduction.

Blockers are often included in the BIOS (Basic Input-Output system - the basic input / output system that is stored on the motherboard chip). Polyphages are the most "heavyweight", they take up a lot of disk space and "eat up" a large amount of RAM.

Varieties of defenses. Depending on the type of threat (known or unknown to specific software), the antivirus can implement proactive or reactive protection:

Proactive protection (heuristics). Protection against unknown viruses based on the study of the code and behavior of programs typical of malware. This type of protection shows the best results when fighting modified viruses. It takes data about already existing threats as a basis. Heuristics in the anti-virus context are a set of rules that are used to detect the actions of malicious programs without the need to identify a specific threat.

Reactive defense (virus signature). Protection against already known viruses based on information about the code and other features of the malware. To work as efficiently as possible, such antiviruses must constantly update their virus signature databases. Protection based on virus signatures involves referring to a dictionary with already known viruses, which were compiled by antivirus software developers.

The main drawback of proactive protection is the so-called "false positives", frequent blocking of uninfected software. The downside of reactive protection is the inability to defend against new threats. Modern antivirus software uses both proactive and reactive protection.

Once the antivirus detects malicious code, it can do the following (depending on the user's settings):

Try to "cure" the infected file by removing the malicious code from it.

Quarantine the infected file. Relevant for files valuable to the user. While in quarantine, an infected file cannot harm your PC; later, it can be cured by yourself or with the help of third-party specialists.

Delete the infected file. If the code cannot be fixed, the file can be permanently deleted from the hard drive.

Take no action. If you suspect a file has been flagged as malicious by mistake, you can add the file to the antivirus exclusions list.

Comprehensive antivirus software always protects your computer in real time. That is, the antivirus is loaded along with the OS, always keeps the RAM and file system of the PC under control, and also monitors all programs that are launched and downloaded. Antivirus software greatly reduces the risk of losing valuable data and also prevents malware from entering your PC. (17)

3.2.3 Methods for testing antivirus programs

Today, in the field of testing software and related products, there are four types of methods at once:

- Static
- Dynamic
- Testing the speed of reaction
- Retrospective

Static testing

It is the simplest and most understandable way to carry out health checks of anti-virus programs and related components. Its essence is based on mandatory scanning on demand, which is reproduced based on the available malware.

For the static test to give definite results, you need to use a massive collection of malwares, the structure of which contains more than a thousand files and related documents.

The network has specialized collections of similar test organizations (AV-Test and AV-Comparatives), which contain more than a thousand of all kinds of programs and files that allow you to perform successful tests. Sometimes the structure of such components can include up to a million files.

Of course, the tests provided have their pros and cons.

On the positive side, the entire testing process is reproduced on many collections of available "harmful" software, which provide the most popular types of malicious content.

The downside is that these collections tend to include only new releases of malicious files. As practice shows, samples with a "life" period of no more than six months are actively used.

In addition, on the negative side, it can be noted that such checks allow you to emulate a hard drive on demand, while in real life the user receives malicious files and elements through a personal email account or via direct download from the global network. It is very important to find such files just now when they appear on the client's personal computer.

Dynamic study

Its main essence is to carry out the process of reproducing a real client environment with the help of the maximum available number of various virtual means, within which the required product is actively tested, which is responsible for the security of the user environment. Such tests are gaining more and more popularity every day due to the rapid

appearance of new properties and methods that are almost impossible to fully implement within a traditional test environment.

For example, to analyze the current effectiveness of the anti-virus protection used, the PC Pro testers did not just reproduce the virus collection on demand, but purposefully downloaded mailing lists with infected files, or, based on written scripts, emulated downloading dangerous files from the Internet.

It is such a test that can be considered the closest to a real situation, and as it became clear, the ability to counteract virus programs and components in most client products turned out to be very lower than the number of viruses found during scanning of infected documents and other files on demand.

Checking the rate of reaction

Although this technique is not very in demand and popular these days, this type of checks should also be detailed and deciphered.

It was the reaction rate testing that was carried out almost every day at a time when the global network was suffering from the "plague of mail worms." You can even recall the name of such programs - Sobig, Bagle, Mydoom, Sober.

Unlike the static type of test, the reaction rate test uses a very small set of required samples.

To accurately determine the reaction rate of the scanned antivirus program, first of all, attention is paid to the speed of detection of the latest modification and assembly of malicious content. By the way, when performing such checks, only those antiviruses remain in preference, the databases of which are most often updated and replenished with new information and protection files.

Conducting a retrospective testing

In complete contrast to the classical methods and methods of verification, retrospective testing provides different versions of anti-virus protection as of the same moment, but in the past.

As a rule, such a moment is very remote from the date of testing, so that the maximum available number of computer viruses that need to be worked on came out. That is, the results of retrospective testing make it possible to assess the real protection of the tested antivirus software product.

Anti-Virus testing by laboratories

Analyzing the results of the inspection by a specialized laboratory, first, it is worthwhile to study in detail the "run-through" product, as well as its supplier.
Indeed, it very often happens that different tests can investigate 2 identical products released by the same developer in different ways. Therefore, it is strongly recommended to conduct a comprehensive research into the technologies of the anti-virus content developer.
A detailed report of such highly specialized laboratories as ICSA and West Coast Labs on the verification of a supplier's product is always published only after testing has ended with an extremely positive rating.

It is the assessments of these laboratories that have recently begun to play an important role in the selection of tested antivirus software, but their absence does not mean that the product is of poor quality or second-rate. The developers just didn't want to participate in the testing process.

Relevance of Anti-Virus testing

Over the past few years, the relevance of countering threats that have not yet been detected has grown significantly. To predict the level of software protection against viruses that have not yet been released, you need to use certain testing techniques. Classic tests are unlikely to help here because they are all, without exception, aimed at the ability to withstand threats that have already been detected by someone earlier.
On the one hand, it is possible to completely disable the signature bases of the tested product and analyze how, without them, it is able to detect malicious components from the modern "In The Wild" list.
But you need to immediately make a reservation that such a technique will not lead to the desired result: the very nature of any antivirus involves working with a signature base.
A protective component with disabled such bases is a completely different product, which makes no sense to test and run.
Of course, you can test the performance of the antivirus to find outgoing viruses in the future by checking the current virus database, but only in the case of working with a signature database that is at least six months old.
It is logical to assume that the viruses that are currently on the ITW list did not exist six months or a year ago. The antivirus component will have to cope with threats that are not yet available on the global network.

By the way, a specialized resource av-comparatives.com works with such checks, where each user can independently get acquainted with the results of retrospective checks, which help to choose the most suitable antivirus, as well as track the trend in the development of security programs and components.

Universal test case Anti-Virus program checks

- Basic test criteria:
- Virus base detection rate
- Detection rate according to the "in the wild" list
- The number of false positives
- Heuristic analysis
- Emulation process

Treatment of the infected component.

Virus base detection rate. When testing an antivirus, an on-demand scan is launched with many infected species. The infection level is directly determined as the percentage of the number of infected components to the total number of tested files.

The "in the wild" detection rate means checking files and components taken from the notorious ITW list. It is determined by the percentage of malware found to the total number of objects.

The number of false positives. For the test, a large number of various files are used, which in their essence are not considered malicious. The check determines the number of false positives to the total number of elements.

Heuristic analysis is a special method entirely based on signatures and heuristics that allows you to effectively find modified versions of viruses when the signature is not 100% identical to the body of an unknown utility, and the suspicious program contains all the signs of a virus component.

This technology, by the way, is rarely used in modern tests, as it can easily increase the percentage of false positives during a run.

Emulator - a large-scale study of a component with a signature scanner for suspicion of the content of a malicious element.

Cure is a method of determining the ability of anti-virus components to "cure" objects when a malicious environment has already reached the user's files and actively prevents its direct removal.

In conclusion, a very accurate conclusion can be made regarding the fact that today there is no 100% effective software component that would quickly and accurately kill and neutralize virus components and data.

But an exceptionally complete understanding of possible threats and the correct selection of anti-virus protection methods can reduce the level of potential infection to a minimum and correctly build the process of testing and analyzing a specific security product. This means that your QA team must approach the testing of antivirus components responsibly and with a clear understanding of what is being done. (18) (19)

4 Practical Part

Oracle VirtualBox virtual machine was installed on the computer to run antivirus tests. Windows 10 64-bit was installed on this virtual machine. Windows has been updated to the latest up-to-date version, as has the VirtualBox.

Antivirus testing process consisted of several stages. First, the latest up-to-date version of the antivirus was downloaded to the virtual machine. After the download of the security software ended, the computer was completely disconnected from the Internet and external USB devices (the exception was a USB flash drive, which contained viruses that were necessary for the test). The next step was to upload viruses to the computer using a USB flash drive. The final and most important stage is testing. After completing the last stage, all steps were repeated anew, but with another antivirus from the list.

4.1 Tested hardware and software

For this test, a computer was selected in the following configuration:

- **Model:** Asus N46VB
- **CPU:** Intel Core i7-3630QM
- **RAM:** 8 GB
- **GPU:** Nvidia GeForce 740M
- **HDD:** 1000 GB
- **Operating system:** Windows 10 Pro 64-bit
- **Virtual machine:** Oracle VirtualBox v.6.1.18 with installed Windows 10 pro 64-bit, 50 GB HDD and 4 GB RAM

4.2 Tested malware

Virus files for testing antiviruses were downloaded from the site where many databases of various viruses located. These sites have different numbers and types of viruses. Viruses can be downloaded one at a time or there are collections of viruses in a zip file. The choice was made in favour of the second option. The virus zip file contained 20 001 malicious programs. Trojan horses and malware were the main contributors, but other types of viruses were more likely to be present. The zip-file was password protected to prevent viruses from spreading all over the computer immediately after downloading. Therefore, the unpacking of this file was carried out only after the virtual machine was downloaded to a personal computer and the Internet was completely disconnected.

During testing, it was revealed that by unpacking the main zip-file, but not moving its contents to the desktop, antiviruses find either very few virus files, or do not find viruses at all. Therefore, it was decided not only to unpack the archive, but also to move the folder with viruses from it, although the instructions on the site where the viruses were downloaded stated that it was enough just to enter the password from the archive and unpack it.

4.3 Test criteria

One criterion was not enough to determine the best antivirus program, since there was a possibility that they might turn out to be the same for several antiviruses, so it was decided to use several evaluation criteria. In addition to the number of successfully found viruses, the time that each security software spent searching for infected files will be considered and used RAM. Based on these factors, the best antivirus was determined.

4.4 Tested antiviruses

The choice of antiviruses was based on their popularity and effectiveness. Many sites, both manufacturers and Internet pages with a rating of this software, were viewed. One of the main selection criteria was also a set of protective functions that would accurately reflect the attacks used when testing viruses.

4.4.1 Kaspersky Free

Kaspersky Free provides comprehensive protection against various types of information threats. To solve complex protection problems, Kaspersky Free includes various protection functions and components.
Protection components are designed to protect your computer in real time from various types of information threats, network attacks, and fraud. Each type of threat is handled by a separate protection component.

Protection components

File Anti-Virus. File Anti-Virus allows you to avoid infecting your computer's file system. The component is launched at the start of the operating system, resides in the computer's RAM and checks all opened, saved and run files on your computer and on all attached disks.

Mail Anti-Virus. Mail Anti-Virus scans incoming and outgoing mail messages on your computer. The letter will be available to the addressee only if it does not contain dangerous objects.

Web Anti-Virus. Web Anti-Virus intercepts and blocks the execution of scripts located on websites if these scripts pose a threat to the computer's security. Web Anti-Virus also monitors all web traffic and blocks access to dangerous sites.

IM Anti-Virus. IM Anti-Virus ensures the safety of working with IM clients. The component protects information coming to your computer via IM client protocols. IM Anti-Virus ensures safe operation with many instant messaging programs.

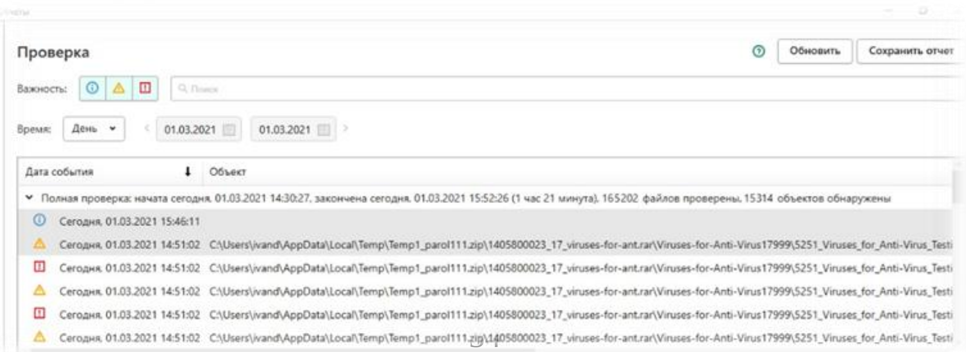
Anti-Phishing. Anti-Phishing allows you to check web addresses for belonging to the list of phishing web addresses.

Activity monitoring. The System Watcher component cancels changes in the operating system caused by malicious and other application activity.

Protection against network attacks. The Network Attack Blocker component is launched at the start of the operating system and monitors incoming traffic for activity typical of network attacks. (20)

Test

Kaspersky Free anti-virus software was the first object of testing. Before starting the scan, all available updates recommended by Kaspersky lab were downloaded and installed on the computer intended for testing. Antivirus version 21.2.16.590 was used for the test. This version took up 214.3 megabytes of computer RAM. To diagnose the computer, the full computer scan mode was selected. For the reliability of the test, the laptop was disconnected from the Internet. A full scan of the tested computer detected 15 314 infected files, while the total number of viruses located on the computer was 20 001. This is equal to 76.57 % of the total number of detected viruses. Full testing took 1 hour and 21 minutes. During this time, 165 202 files on the hard drive were scanned. The scanning speed of Kaspersky Free antivirus software was 33.99 files per second.



pic. 1 - Kaspersky test results

Name	Kaspersky Free
Version	21.2.16.590
Number of detected Viruses	15 314
Percentage of detected viruses	76.57
Scan time (hh:mm:ss)	01:21:00
Scan speed (files per second)	33.99
Number of scanned files	165 202
Used RAM (MB)	214.3

Table 1 - Kaspersky test results

4.4.2 Avira Free Antivirus

Avira Free Antivirus is a free antivirus, anti-spyware, and anti-rootkit with cloud technology to protect against the known, latest and most sophisticated threats.
Antivirus offers basic protection against malware, but can be enhanced with free apps and services from Avira, including the addition of Internet protection, parental control and Android protection, which helps protect your computer, sensitive information, mobile devices and children from all kinds of online threats.

Main features of Avira Free Antivirus

Antivirus and antispyware. Effective protection in real time and on demand against various types of malware: viruses, Trojans, Internet worms, spyware and adware. Constant automatic updates and AHeAD heuristic technology reliably protect against known and new threats.

Cloud protection. Avira Protection Cloud - real-time threat classification and fast system scans.

Rootkit protection. Avira Anti-Rootkit protects against difficult-to-detect threats - rootkits.

Windows Firewall Control. Avira Free Antivirus allows you to edit network rules for applications, change network profiles (Private, Public) and manage advanced settings for Windows Firewall with Advanced Security.

Internet protection. Safe search, block phishing and malicious websites, anti-tracking. This feature is part of the Avira Browser Safety toolbar for Chrome, Firefox and Opera browsers (installed separately from Avira Free Antivirus).

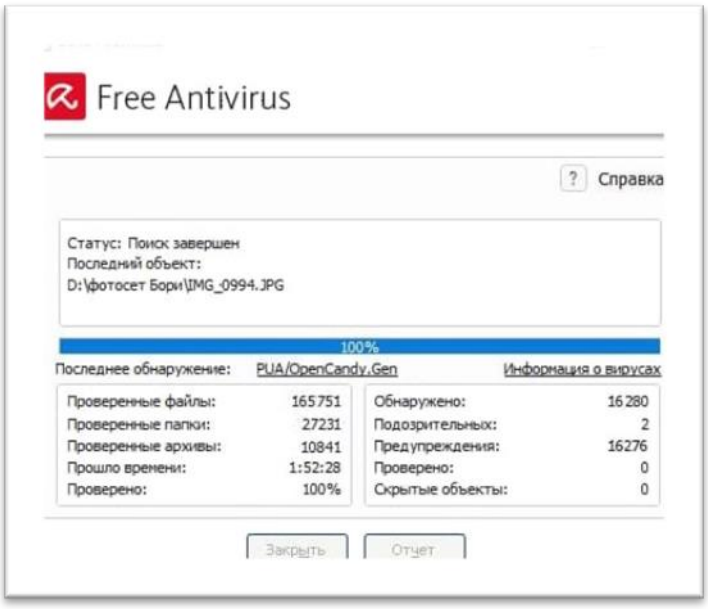
Parental control. With the Social Networking function, based on Avira Free SocialShield technology, it is possible to monitor the activities of children on the Internet: checking social network accounts for comments, photos, etc. that could negatively affect the child. (21)

Test

Avira Free antivirus has proven to be very good at finding viruses. While scanning the computer, the security program detected 16 280 malicious files, if we translate the result into a percentage, it is 81.4%. It took the antivirus program 1 hour 52 minutes and 28 seconds to scan the entire system. It took Avira antivirus so long to scan 165,751 computer files. Knowing how many files were scanned and how much time was spent on this process, it becomes possible to determine how many files the antivirus can scan in a second and it is 24 files in one second. It should be noted that this antivirus was updated to the latest up-to-date version before the test.

Name	**Avira Free Antivirus**
Version	1.0.45.15812
Number of detected Viruses	16 280
Percentage of detected viruses	81.4
Scan time (hh:mm:ss)	01:52:28
Scan speed (files per second)	24
Number of scanned files	165 751
Used RAM (MB)	205.2

Table 2 - Avira test results



pic. 2 - Avira test results

4.4.3 Bitdefender Antivirus Free Edition

Bitdefender Antivirus Free Edition is a free antivirus that uses Bitdefender's virus signatures and proactive technologies to protect against new and unknown threats in real time.

The functionality and efficiency of full-fledged paid solutions allows you to reliably protect your computer from malware, network threats, fraudulent and phishing websites.

The payback for being free is the inability to customize protection for a specific security level. At the same time, it makes the solution simple and easy to use for ordinary computer users.

Key features of Bitdefender Antivirus Free Edition

Real-time protection. The real-time screen provides protection during access. All files are scanned now they are started or copied. For example, files you just downloaded from the Internet are scanned immediately.

Cloud Technologies - Bitdefender Antivirus Free Edition uses cloud scanning to accelerate detection and reveal new or unknown threats that other antivirus programs miss.

Active Virus Control is an innovative proactive detection technology that uses advanced heuristic methods to identify new potential threats in real time.

HTTP Scan - Bitdefender's free antivirus analyses and blocks fraudulent and phishing websites.

Anti-rootkit - a technology used to search for hidden malware, also known as rootkits.

Periodic Updates - Bitdefender Antivirus Free Edition is periodically updated without user intervention to provide the optimal level of protection against new threats.

Early Scan at System Boot - This technology ensures that the system is scanned at boot time as soon as all important services are running. It allows you to improve the detection of viruses at system start-up, as well as speed up the boot time.

Scanning while idle - Bitdefender's free antivirus detects when the use of computer resources is minimal so that it can scan the system without affecting user activity. System resource utilization is calculated based on processor (CPU) and hard disk (HDD) utilization.

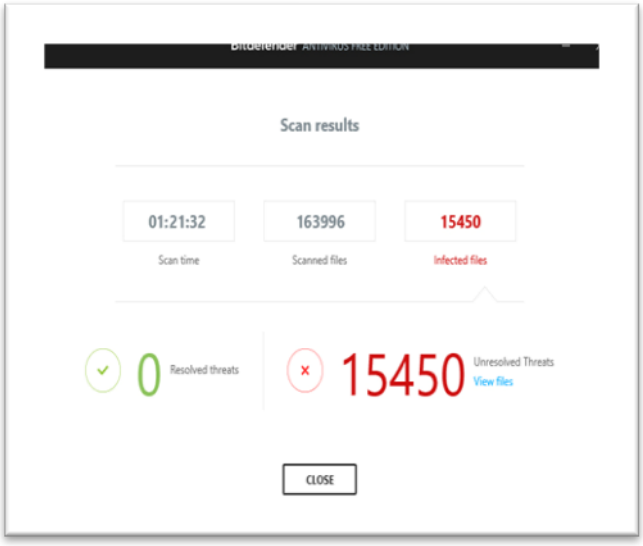
Smart Scan technology - files that were previously scanned by Bitdefender Antivirus Free Edition will not be scanned again using the smart file scan skip engine. (22)

Test

Bitdefender Antivirus Free Edition passed the test in 1 hour 21 and 32 seconds. In total, the antivirus scanned 163 996 system files. During the full cycle of scanning the operating system of the computer, 15 450 were found, which is 77.25 %. The speed at which the security software scanned the computer's hard drive was 33.5 files per second. The antivirus has been updated to the latest version, with Bitdefender taking up 176.3 megabytes of RAM.

Name	**Bitdefender Antivirus Free Edition**
Version	1.0.21.225
Number of detected Viruses	15 450
Percentage of detected viruses	77.25
Scan time (hh:mm:ss)	01:21:32
Scan speed (files per second)	33.5
Number of scanned files	163 996
Used RAM (MB)	176.3

Table 3 - Bitdefender test results



pic. 3 - Bitdefender test results

4.4.4 Avast Free Antivirus

Avast Free Antivirus - ultra-light and modern protection with minimal strain on system resources.

Free Avast Antivirus has been enhanced to improve efficiency and reduce the strain on computer's system resources.

Main components of Avast Free Antivirus:

- Antivirus and antispyware
- Behavior analysis
- Protection against ransomware
- CyberCapture
- Web protection
- Mail protection
- Wi-Fi network analysis
- Password manager

Main features of Avast Free Antivirus

- Intelligent scanning. Detection of all vulnerabilities that could allow malware to enter the system: from insecure passwords to suspicious add-ons and outdated software.
- Antivirus. Detect and block viruses, malware, phishing, spyware, and ransomware.
- Protection against ransomware. Block untrusted applications and ransomware from modifying, deleting, or encrypting personal photos and files.
- Behavior analysis. Detect suspicious behavior instantly to protect against ransomware and zero-day threats.
- Web protection and phishing protection. Protection from malicious sites, fraudsters and preventing the transition to fake sites without installing a special browser extension.
- Mail protection. Prevents infected emails from entering your mailbox on a computer, such as Outlook and Thunderbird, and prevents the sending of infected emails from your account.
- Network analysis. Automatically detects weak spots in your home Wi-Fi network to protect it from intruders.

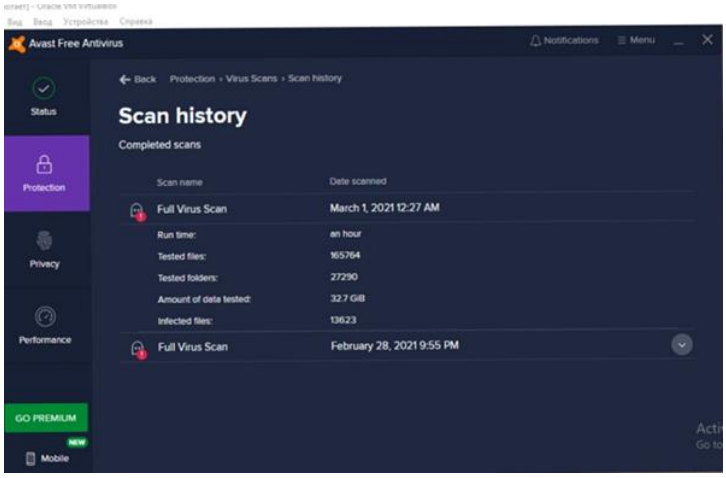
- Password manager. Protect all accounts with one strong password. You will be able to use the new passwords we created for secure authorization. (23)

Test

Based on the test results, Avast Free Antivirus software version 21.2.16.590 found 13 623 infected files or 68.11 percent of found viruses. For 1 hours 165 764 files were scanned. This means that this antivirus program diagnoses 46 files per second. The amount of occupied RAM on the computer by the Avast Free antivirus is 142.7 megabytes. Full scan of all files was selected from the offered scan options. Scanning was started manually. It is also worth noting that this software was updated to the latest available version at the time of the test launch, via the Internet. At the time of the scan, the computer was disconnected from the Internet so that the virus files would not be able to contact the server. All information about antivirus software, version and testing parameters have been moved to the table.

Name	**Avast Free Antivirus**
Version	21.2.16.590
Number of detected Viruses	13 623
Percentage of detected viruses	68.11
Scan time (hh:mm:ss)	01:00:00
Scan speed (files per second)	46
Number of scanned files	165 764
Used RAM (MB)	142.7

Table 4 - Avast test results

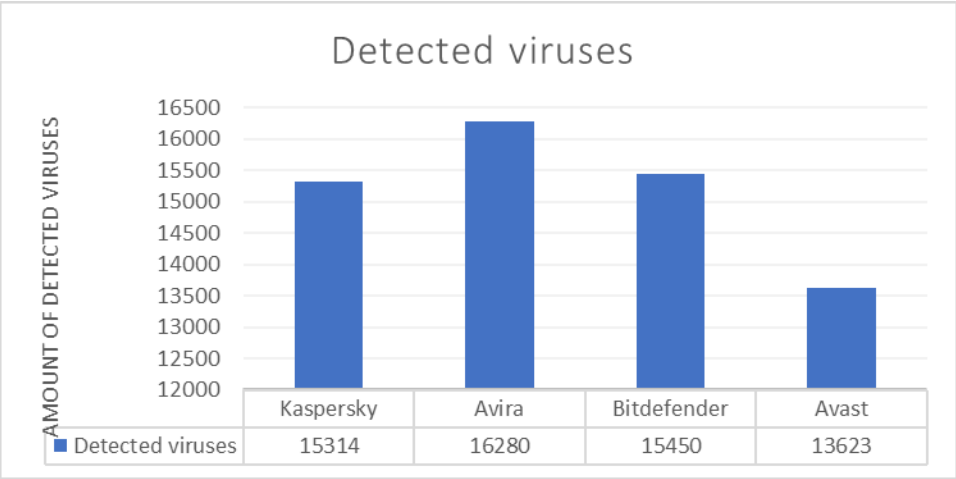


pic. 4 - Avast test results

5 Results and Discussion

5.1 Amount of detected viruses

Antivirus testing showed that Avira Free Antivirus was able to identify the most viruses. During the full scan of the computer, the antivirus found 16,280 viruses, which is 81.4 percent of the successful detection of malicious programs. Bitdefender Antivirus Free Edition came in second. The antivirus identified 15,450 virus files. This number is 830 less viruses than the previous antivirus detected. If we convert this number into percent, then it will amount to 77.25 successfully identified viruses. In third place, with a small lead over competitors, is Kaspersky Free. The antivirus program was able to find 15,314 viruses, and the percentage of malware is 76.57, it was 0.63 percent less than Bitdefender. As you can see in the picture number 5, Avast Free Antivirus is in last place with a score of 13,623 files. This is 68.11 percent of the viruses found.

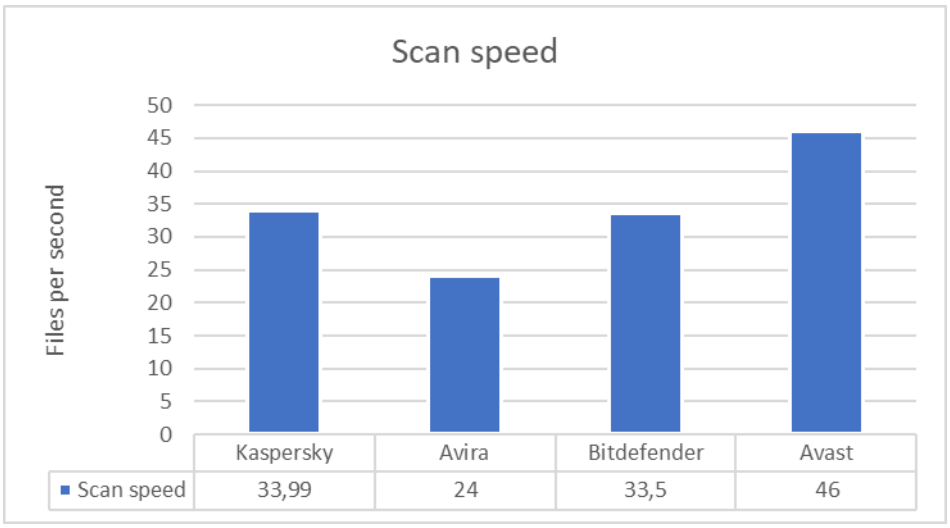


pic. 5 - Detected viruses

5.2 File scan speed

One of the important criteria in determining the best one was the maximum speed at which antivirus programs can scan the system. The unit of measurement was the number of files scanned in one second. Avast Free Antivirus ranked first in this test with 46 scanned files in one second. The leader is followed by Kaspersky Free with a score of 33.99 files per second. Bitdefender Antivirus Free edition is in third place with a very small gap. It was able to scan 33.5 files scanned in one second. And in last place is Avira Free Antivirus with the

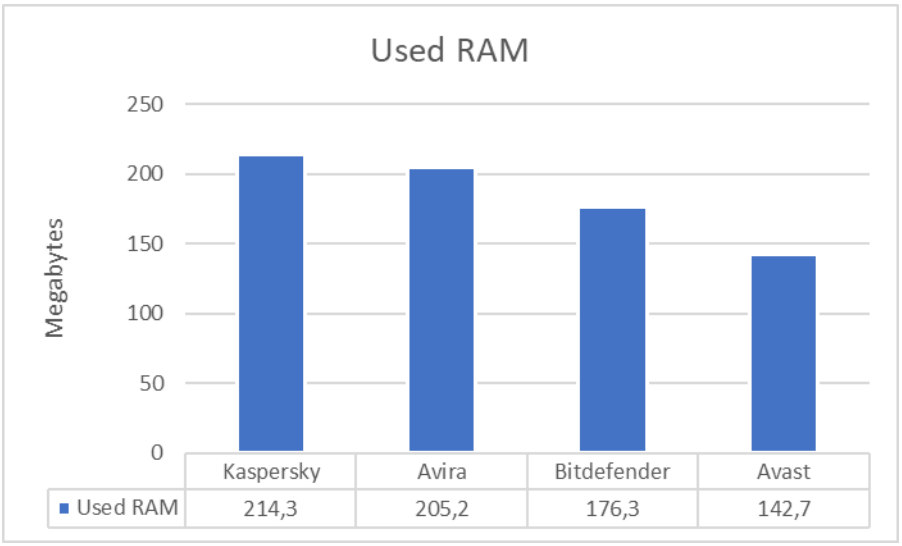
results of 24 files scanned in one second. The results of all antiviruses can be seen in the picture under the number 6.



pic. 6 - Scan speed

5.3 Used RAM

Avast Free Antivirus ranks first. It took up the least amount of RAM on a personal computer. It used 142.7 megabytes. Next is Bitdefender Antivirus Free Edition with 176.3 megabytes of RAM, which is 34.5 megabytes more than the previous antivirus. In third place is Avira Free Antivirus. As you can see in the picture number 13, the antivirus program used 205.2 megabytes of RAM. Most of the RAM was occupied by the antivirus Kaspersky Free it was 214.3, so it took the last place.



pic. 7 - Used RAM

5.4 Antivirus software for home personal computers

Choosing the best security software is the main goal of this bachelor thesis. Obviously, one of the tasks of an antivirus program is to protect a personal computer from viruses, which includes saving important data for the user.

The testing of the selected antiviruses was carried out on the personal computer of an ordinary user. Therefore, in the first place, the antivirus program that is best suited for protecting home computers will be selected.

The choice of antivirus will be carried out according to the already established criteria, namely: the number of detected viruses, the speed of scanning files and the amount of used RAM.

5.4.1 Home personal computers

Antivirus scores will be distributed as follows. In the first place, without any doubt, should be the number of detected viruses, since the most critical point. It will account for 50% of the total score. File scanning speed will have 25 percent, because all users are interested in scanning not only with high quality, but also fast. RAM also gets 25 percent, because even if this is the most reliable and fastest protection, but which greatly overloads RAM, this can negatively affect the experience of using this program. Based on the results of multi criteria analysis available in Table 7, Bitdefender Antivirus Free Edition came out on top. The total score of this security software is 0.58, which is only 0.05 hundredths more than Avira Free Antivirus, which came in second. Min-max formula was used for calculations. The formula is $x' = (x - \min(x)) / (\max(x) - \min(x))$. Also, unweighted normalized score avaliable in table 6.

Antivirus name	Percentage of detected viruses	Used RAM (MB)	Scan speed (Files/second)
Kaspersky	76.57	214.3	33.99
Avira	81.4	205.2	24
Bitdefender	77.25	176.3	33.5
Avast	68.11	142.7	46

Table 5 - Overall test results

Unweighted normalized score			
Antivirus name	**Detected viruses**	**Used RAM**	**Scan speed**
Avira	0,64	0,00	0,45
Bitdefender	1,00	0,13	0,00
Avast	0,00	1,00	1,00
Weight	0,5	0,5	0,25

Table 6 - Unweighted normalized score

Weighted normalized score				
Antivirus name	**Detected viruses**	**Used RAM**	**Scan speed**	**Total score**
Kaspersky	0,32	0,00	0,11	0,43
Avira	0,50	0,03	0,00	0,53
Bitdefender	0,34	0,13	0,11	0,58
Avast	0,00	0,25	0,25	0,50
Weight	0,5	0,25	0,25	

Table 7 - Multi criteria analysis results

6 Conclusion

This bachelor thesis is called "Information Security", so the main goal of this work was to find software that would best cope with protecting users' personal data from virus programs.

To choose the best antivirus, special criteria were set: the number of viruses found, the testing speed and the amount of used RAM. The better the antivirus performed according to the selected criteria, the higher the position it occupied.

Avira Free Antivirus ranked first in terms of the number of detected viruses with 81.4 percent of successfully detected virus files. Bitdefender Antivirus Free Edition came in second with 77.25 percent of scan success. The third place was given to Kaspersky Free, which received 76.57 percent, which is not much less than the antivirus in second place. And in fourth place is Avast Free Antivirus, which was only 68.11 percent successful in finding infected files.

When comparing the speed of scanning files, the places were distributed differently. Avast Free Antivirus was able to scan the largest number of files. Its result was 46 scanned files in one second. The second was Kaspersky Free with a score of 33.99. Bitdefender Antivirus Free Edition is not far behind. Its scan rate was 33.5 files per second. And in fourth place was Avira Free Antivirus, with 24 files.

In terms of the amount of used RAM, Avast Free Antivirus showed the best results with a result of 142.7 megabytes. The second place went to Bitdefender Antivirus Free Edition. Its result is 176.3 megabytes of RAM. The third place got Avira Free Antivirus with 205.2 megabytes of used RAM. With a score of 214.3 megabytes, Kaspersky Free took fourth place.

The results of the multi criteria analysis showed that when considering all the results listed above (table number 5), Bitdefender Antivirus Free Edition is the best antivirus. However, the advantage of this antivirus is not obvious in comparison with competitors.

7 References

1. **Stroll, Clifford.** *The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage.* New York City : s.n., 2055. ISBN: 1416507787.
2. **Sahay, Manish.** Who Invented the Antivirus? A History of Antivirus Software. *ThePCinsider web site* . [Online] ThePCinsider, October 08, 2020. https://www.thepcinsider.com/who-invented-antivirus-history-timeline-evolution/.
3. **Blokdyk, Gerardus.** *Antivirus software: A Complete Guide.* s.l. : CreateSpace Independent Publishing Platform, 2018. ISBN-13: 978-1718608214.
4. **Malwarebytes support.** Malwarebytes: Computer virus. *Malwarebytes web site.* [Online] Malwarebytes, February 23, 2021. [Cited: January 11, 2021.] https://www.malwarebytes.com/computer-virus/.
5. **Avira support.** Avira Free Antivirus for Windows. *Avira web site.* [Online] Avira, March 2, 2021. [Cited: February 3, 2021.] https://www.avira.com/en/free-antivirus-windows.
6. **Bitdefender.** Bitdefender Antivirus Free Edition. *Bitdefender web site.* [Online] Bitdefender, March 1, 2021. [Cited: January 3, 2021.] https://www.bitdefender.com/solutions/free.html#.
7. **Cisco Security.** *Cisco web site.* [Online] Cisco Company, June 14, 2018. [Cited: March 1, 2021.] https://tools.cisco.com/security/center/resources/virus_differences#spyware.
8. acsedu. Computer Bugs and Viruses. *acsedu web site.* [Online] acsedu, March 6, 2021. [Cited: November 12, 2020.] https://www.acsedu.co.uk/Info/Computers/Computer-Servicing/Computer-Bugs-and-Viruses.aspx.
9. Webroot. Cybersecurity Resources Tips: Articles What are Bots, Botnets and Zombies? *Webroot web site.* [Online] Webroot, August 3, 2020. [Cited: March 2, 2021.] https://www.webroot.com/us/en/resources/tips-articles/what-are-bots-botnets-and-zombies.
10. Avast. Free antivirus is your first step to 3D online protection. *Avast web site.* [Online] Avast, July 12, 2020. [Cited: March 5, 2021.] https://www.avast.com/en-us/.
11. Microsoft support. Rootkits malware. *Microsoft web site.* [Online] Microsoft, January 1, 2020. [Cited: March 5, 2020.] https://docs.microsoft.com/en-us/windows/security/threat-protection/intelligence/rootkits-malware.
12. Michael Veenstra. Trending 'Fireball' adware raises botnet concerns. *BetaNews web site.* [Online] BetaNews, July 6, 2017. [Cited: January 5, 2021.] https://betanews.com/2017/06/14/trending-fireball-adware-raises-botnet-concerns/.
13. Crowdstrike. Types of Malware. *The 11 most common types of malware.* [Online] Crowdstrike, June 12, 2020. [Cited: January 23, 2021.] https://www.crowdstrike.com/cybersecurity-101/malware/types-of-malware/.
14. Dell support. What are the different types of Viruses, Spyware and Malware that can infect my computer? *Dell web site.* [Online] Dell , May 3, 2020. [Cited: March 5, 2021.] https://www.dell.com/support/kbdoc/cs-cz/000132699/what-are-the-different-types-of-viruses-spyware-and-malware-that-can-infect-my-computer?lang=en.
15. McAfee, LLC. What Is ransomware? *McAfee web site.* [Online] McAfee, LLC, April 3, 2020. [Cited: March 5, 2021.] https://www.mcafee.com/enterprise/en-us/security-awareness/ransomware.html.
16. Nica Latto. Worm vs. Virus: What's the Difference? *AVG web site.* [Online] AVG, December 18, 2020. [Cited: February 5, 2021.] https://www.avg.com/en/signal/computer-worm-vs-virus.
17. Balaban, David. 17 types of Trojans and how to defend against them. *csoonline web site.* [Online] CSO, January 14, 2021. [Cited: march 1, 2021.] https://www.csoonline.com/article/3602790/17-types-of-trojans-and-how-to-defend-against-them.html.

18. Kaspersky Lab support. Malware & Computer Virus Facts & FAQs. *Kaspersky Web site.* [Online] Kaspersky Lab, May 6, 2019. [Cited: August 5, 2020.] www.kaspersky.com/resource-center/threats/computer-viruses-and-malware-facts-and-faqs.
19. TestMatick. Methods of testing the antiviruses . *TestMatick web site.* [Online] TestMatick, August 13, 2018. [Cited: September 9, 2020.] https://testmatick.com/methods-of-testing-antiviruses/.
20. Rubenking, Neil J. How We Test Antivirus and Security Software. *PCMag website.* [Online] PCMag, October 7, 2019. [Cited: March 3, 2021.] https://www.pcmag.com/news/how-we-test-antivirus-and-security-software.
21. Prince, Brian. CryptoWall Ransomware Cost Victims More Than $18 Million Since April 2014: FBI. *securityweek.* [Online] securityweek, June 154, 2015. [Cited: November 21, 2020.] https://www.securityweek.com/cryptowall-ransomware-cost-victims-more-18-million-april-2014-fbi.
22. Norton. What Is Adware? *Norton web site.* [Online] Norton, May 3, 2019. [Cited: February 3, 2021.] https://us.norton.com/internetsecurity-emerging-threats-what-is-grayware-adware-and-madware.html.
23. support, Kaspersky. Kaspersky Free Antivirus. *Kaspersky web site.* [Online] Kaspersky Lab, March 1, 2021. [Cited: March 4, 2021.] https://www.kaspersky.com/free-antivirus.