ETHIOPIAN INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH

eISSN: 2349-5715 pISSN: 2349-5707

Volume: 11, Issue 06, June-2024 SJIF 2019: 4.702 2020: 4.737 2021: 5.071 2022: 4.919 2023: 6.980 2024: 7,662

ANALYSIS OF ANTIVIRUS PROGRAMS' EFFECTIVENESS

Anvar Aytanov, Ph.D., teacher of the Department of Information,

Duysenbaeva Dilfuza Sharapatdinovna[2],

Baxitjanova Kamshat Jambil qizi[3]

[1]A teacher of The Department of Information Security
[2]A student of The Department of Information Security
[3]A student of The Department of Information Security

Annotation: In this article, the meaning of computer viruses is studied, distinguishing their main characteristics and classifying them according to various criteria. Beyond this, methods of combating computer viruses, requirements for antivirus programs, their characteristics, and ways to ensure security are discussed along with their effectiveness.

Keywords: antivirus, virus, infection method, bootloader.

At present, the secure implementation of information technologies and computer systems, as well as ensuring data integrity, is highly relevant. The persistent threat of computer viruses, which are increasingly sophisticated and malicious, poses significant risks for users and organizations alike. Effective combat against these threats often relies heavily on the widespread use of antivirus programs.

A computer virus is a malicious program designed by malicious programmers to infiltrate computer systems, replicate itself, and spread its code. This harmful code can often operate stealthily and become active without the user's knowledge. Understanding the main objectives, infection methods, and characteristics of viruses allows us to:

Viruses typically consist of two main components: a bootloader and a self-replicating module. The bootloader is responsible for initiating the virus within the system and determining how it spreads, while the self-replicating module handles the replication of the malicious code.

Viruses use various methods to infiltrate systems, including malicious email attachments, harmful websites, USB flash drives, among others. Additionally, they can camouflage themselves within legitimate files to evade detection by antivirus programs.

Viruses have different objectives depending on their design, ranging from disrupting data to stealing information. Some viruses create backdoors for hackers to gain unauthorized access to compromised systems, while others aim to encrypt data for ransom or disrupt computer operations. Computer viruses come in various types, and they can be classified according to different criteria:

By Infection Method:

- File Viruses: These infect executable files.
- Boot Sector Viruses: They target the boot sector of storage devices.
- Macro Viruses: They infect documents and electronic spreadsheets by exploiting macros.

By Impact Objective:

- Destructive Viruses: These aim to delete or corrupt data.
- Stealth Viruses: They hide themselves to evade detection.
- Botnet Viruses: These viruses aim to create networks of infected computers (botnets) that can be controlled remotely for various malicious purposes.

eISSN: 2349-5715 pISSN: 2349-5707
Volume: 11, Issue 06, June-2024 SJIF 2019: 4.702 2020: 4.737 2021: 5.071 2022: 4.919 2023: 6.980 2024: 7,662

Computer viruses require an understanding of their types to effectively combat them. Knowing the classification of viruses enhances the ability to mitigate their impact on computer systems and provides opportunities for prevention and detection. Below is detailed information about effective methods to combat viruses:

- Utilizing current antivirus programs: Using up-to-date antivirus programs is crucial as they continuously evolve and are equipped with effective defense mechanisms. These programs scan the system for viruses and block their malicious activities.
- Software and operating system updates: Regularly updating all software and the operating system is essential. This ensures that vulnerabilities are patched, making it harder for viruses to exploit weaknesses.
- Configuring firewall settings: Firewall configuration in software and hardware helps control network traffic and prevents unauthorized access. Properly configuring firewalls with caution ensures unnecessary traffic is blocked and enhances system security.
- Filtering email: Implementing email filtering mechanisms helps prevent malicious attachments and phishing emails from reaching the inbox. Such filters reduce the risk of opening infected files or falling victim to phishing attempts.

Combining these methods forms a robust defense strategy for maintaining the stability and security of computer systems against various malware threats.

Antivirus programs play a crucial role in detecting and protecting against viruses, trojans, spyware, and other malicious software. They employ various sophisticated techniques to identify malicious programs and combat them effectively. Many antivirus programs operate in real-time, continuously monitoring the system for viruses and providing immediate protection. Additionally, scheduled scans further ensure that users can detect and address potential threats promptly.

Selecting and utilizing an antivirus program should be tailored to individual needs, the characteristics of the computer system, and its security requirements. An effective antivirus program must meet several critical criteria to provide comprehensive protection and meet diverse demands. In this article, we will now examine the capabilities, usability, advantages, and limitations of various types of antivirus programs for computer system security:

Bitdefender Total Security

Bitdefender stands out in antivirus protection with its robust detection capabilities and features that set it apart from other antivirus programs. When you start using Bitdefender, it initiates quick and thorough scans of your system to ensure comprehensive security. It effectively identifies and blocks malicious files before they can cause harm, and it enhances browsing safety by detecting and blocking web trackers. Additionally, it provides a stringent warning if you attempt to access a potentially dangerous or phishing website without proper caution.

Bitdefender's suite is well-rounded with advanced security features, including secure banking tools, VPN for secure browsing, social media protection, file encryption, parental controls, and more, available in their Total Security package. Moreover, Bitdefender adapts well to individual needs with easy integration across Windows, Mac, Android, and iOS devices, making it a versatile choice for comprehensive protection.

Furthermore, Bitdefender offers flexible licensing options, such as multi-device licenses (up to 10 devices), ensuring convenient coverage for all your devices under one plan.

Technical specifications	**Operating system:** Windows, Mac, Android, iOSMaximum devices covered: 10 **Stand out features**: Safepay bank security, security with several levels, VPN

	Refund period: 30 days **Free trial:** 30 days
Cost	**Bitdefender Antivirus Plus**: $19.99/360 Total Security Free **Bitdefender Antivirus Plus**: €15.99/year
Advantages	+ Has a lot of functions + Security against harmful apps + Special interface + Cost
Disadvantages	- It is possible to use scanners slowly - VPN utilization methods - Current virus protection

Norton 360 Select with LifeLock

Norton excels with its effective protection and consistently achieves high scores in independent security tests. It supports all major operating systems, allowing you to secure every device and gadget in your household that connects to the internet. Without compromising on performance, Norton provides comprehensive defense against malware, cyber threats, and harmful URLs, regardless of where you browse online.

By leveraging data from their vast threat database, Norton can proactively block malicious programs and cybercriminals' attempts, including harmful URLs. Tests from AV-Comparatives confirm Norton's ability to detect and block malware effectively while also offering advanced features like Insight for identifying suspicious activities and files on your system, particularly useful for users with technical expertise. Norton is known for its user-friendly interface and robust protection against emerging types of malware.

Technical specifications	**Operating system:** Windows, Mac, Android, iOS options **Maximum devices covered:** 5-10 **Stand out features:** Virtual security wall, technical support for computers, along with online storage, together form a backup system. **Refund period:** 60 days **Free trial:** 7 days
Cost	**Norton AntiVirus Plus:** $19.99/year **Norton 360 Standard**: $39.99/year **Norton 360 Standard:** £14.99/mth
Advantages	+ Protecting sensitive information from URL access + Secure VPN
Disadvantages	- Job queues are processed in batches after the deadline. - Anonymous VPN usage option - File encryption is absent

Avast One

Avast One is Avast's latest security solution, equipped with comprehensive defenses and features designed for effective and user-friendly protection against all types of malware and threats. It offers seamless integration across Windows, Mac, Android, and iOS platforms, ensuring versatile use across all your devices.

Avast One's scanning speed is moderate, typically taking about 32 minutes to scan 50 GB of files, making it suitable for thorough protection without excessively impacting system performance. Its scanning methods are optimized and allow you to customize scans based on your specific security needs, ensuring comprehensive protection.

The Smart Scan feature quickly checks for malware and suspicious browser extensions in seconds, while Targeted Scans allow detailed examination of selected folders and files for deeper security checks on your system.

Technical specifications	**Operating system:** Windows, Mac, Android, iOS options **Maximum devices covered:** Up to 30 **Stand out features:** VPN, security wall, malicious URL blocker, and password manager. **Refund period:** 30 days **Free trial:** Free version available
Cost	**Avast One Individual:** $29.99/year **Avast One Family:** $69.48/year **Avast One Individual:** £39.99/year
Advantages	+ Protection against malicious software + Comprehensive security protocols implemented
Disadvantages	- Blocking unnecessary add-ons - Excessive VPN charges incurred - Excessive version use

McAfee+ Premium

McAfee + enhances the capabilities of McAfee Antivirus Plus and Total Protection packages by providing robust defenses against standard malware threats and essential features for personal online security.

McAfee + Essential, available for a subscription of 5 devices, offers protection across all major platforms including Windows, Mac, Android, iOS, and Chromebook. While primarily an advanced antivirus program, it also includes features such as comprehensive data monitoring, password manager, firewall protection, file shredder, and secure VPN access.

Technical specifications	**Operating system:** Windows, Mac, iOS, Android **Maximum devices covered:** 10 **Stand out features:** VPN, spam filter, virtual security wall, ID protection **Refund period:** 30 days **Free trial:** 30 days
Advantages	+ Many functions + Secure usage facilitated by VPN + Implements rules for protecting sensitive information
Disadvantages	- Antivirus does not operate on macOS. - The cost is quite high.

F-Secure Total

F-Secure stands out in antivirus protection with its ability to effectively detect and block malware while consuming minimal system resources. Its notable feature lies in its advanced protection against emerging threats.

Internet security is crucial for safeguarding your online activities, transactions, and Wi-Fi connections from potential threats and suspicious activities. Ultimately, this proactive approach helps prevent hackers from exploiting vulnerabilities and causing real harm to your digital environment.

Technical	**Operating system:** Windows, Mac, Android, iOS

eISSN: 2349-5715 pISSN: 2349-5707
Volume: 11, Issue 06, June-2024 SJIF 2019: 4.702 2020: 4.737 2021: 5.071 2022: 4.919 2023: 6.980 2024: 7,662

specifications	**Maximum devices covered:** 10 **Standout features:** Proactive protection, remote management, VPN **Refund period:** 30 days **Free trial:** 30 days
Cost	**F-Secure Total:** $109.99/year **F-Secure Total:** €99/year **F-Secure Total:** £79.99/year
Advantages	+ Comprehensive protection + Blocking of malicious programs + Continuous monitoring and support
Disadvantages	- Not the best option for new users - Does not work with Chromebooks

CONCLUSION

In this article, the intricacies of computer virus management and defense strategies were thoroughly analyzed. Computer viruses pose a significant threat to information systems, potentially leading to critical consequences for computer data and functionality. Therefore, a robust security strategy involving the use of antivirus programs is essential.

The article covered various aspects, starting from understanding the objectives and classification of computer viruses to methods for detecting and defending against them. Antivirus programs employ techniques such as signature-based scanning, heuristic analysis, real-time monitoring, and other advanced methods to ensure comprehensive protection. Key requirements for effective antivirus programs include seamless integration into systems, efficient detection of malicious code, minimal performance impact, and compatibility with diverse operating systems. These programs are designed to safeguard against emerging threats while maintaining operational efficiency and system integrity.

The integration of functions like antispam and antispyware enhances the capabilities of antivirus programs, making them more effective in ensuring comprehensive security and protecting against a wide range of threats. These technologies and proactive defense strategies have evolved over time to adapt to the changing landscape of cybersecurity challenges.

However, effectively combating computer viruses requires more than just selecting antivirus programs. It necessitates seamless integration of security measures, adherence to cybersecurity best practices by users, and the cultivation of a robust cybersecurity culture across information spaces. This holistic approach is crucial for safeguarding against evolving threats and maintaining information security standards.

REFERENCES:

1. Kaspersky, E. M. "Security in Information Technologies. Lecture Course." - Moscow: Piter, 2018.
2. Gudin, S. M. "Information Protection in Computer Systems and Networks." - Moscow: BHV-Peterburg, 2019.
3. Schneider, D. "Secrets of Antivirus Programs. How to Ensure Computer Security." - Moscow: DMK Press, 2017.
4. Bryusov, A. A. "Antivirus Programs. Problem Setting and Solution Methods." - St. Petersburg: BHV-Peterburg, 2018.
5. Gostev, A. V. "Computer Viruses and Antivirus Protection." - Moscow: Piter, 2020.
6. Makeev, A. I. "Information Security. Antivirus Protection." - Moscow: KOLOSS, 2019.