COMPUTER SECURITY, VIRUSES AND INFORMATION PROTECTION METHODS

Mamadaliyeva Hayotxon Xayrullo qizi
Fergana State University Faculty of Foreign Languages
Field of Study: Philology and
Language Teaching (English)
First-year student of group 25.127
Toshboltayev Faxriddin O‘rinboyevich
Scientific Supervisor: Axborot texnologiyalari
kafedrasi katta o‘qituvchisi p.f.b.f.d (PhD)
https://doi.org/10.5281/zenodo.19916107

Annotatsiya: ushbu maqolada kompyuter va axborot xavfsizligi masalalarini batafsil yoritadi. Unda xavfsizlikning kundalik hayotdagi va raqamli muhitdagi ahamiyati tushuntiriladi. Kompyuter viruslari, ularning tarqalishi, tarixi va dunyodagi eng xavfli viruslar misollar bilan bayon etilgan. Shuningdek, zararli dasturlar (malware) turlari, himoya strategiyalari, shifrlashning mohiyati va ishlash mexanizmi, hamda kuchli parol yaratish va brutfors hujumlardan saqlanish bo‘yicha tavsiyalar keltirilgan. Matn kompyuter viruslarining tizimlarga zarar yetkazish usullari va foydalanuvchilarning xavfsizligini ta’minlash choralarini tushuntiradi, axborot xavfsizligi bo‘yicha umumiy bilimlarni oshiradi.

Kalit so’zlar:kompyuter xavfsizligi,axborot xavfsizligi,kompyuter viruslari,zararli dasturlar (malware),antivirus dasturlar,shifrlash (encryption),parol xavfsizligi,global Internet tarmog‘i,tizimni himoya qilish

Аннотация: в данной статье подробно рассматривается компьютерная и информационная безопасность. Объясняется важность безопасности в повседневной жизни и в цифровой среде. Описываются компьютерные вирусы, их распространение, история и самые опасные вирусы в мире с примерами. Также предоставляется информация о типах вредоносного ПО, стратегиях защиты, природе и механизме шифрования, а также рекомендации по созданию надежных паролей и защите от атак методом перебора. В тексте объясняется, как компьютерные вирусы повреждают системы, и приводятся меры по обеспечению безопасности пользователей, а также расширяются общие знания в области информационной безопасности.

Ключевые слова:компьютерная безопасность, информационная безопасность, компьютерные вирусы, вредоносное ПО, антивирусные программы, шифрование, безопасность паролей, глобальный Интернет, защита системы.

Annotation:this article covers computer and information security in detail. It explains the importance of security in everyday life and in the digital environment. Computer viruses, their spread, history, and the most dangerous viruses in the world are described with examples. It also provides information on types of malware, protection strategies, the nature and mechanism of encryption, as well as recommendations for creating strong passwords and protecting against brute force attacks. The text explains how computer viruses damage systems and measures to ensure user safety, and increases general knowledge of information security.

Key words:computer security, information security, computer viruses, malware, antivirus programs, encryption, password security, global Internet, system protection

Security is an aspect of our daily life that we constantly encounter: we lock doors, hide valuable items from strangers’ eyes, and never leave our wallets unattended. This principle must also apply to the "digital world," because every computer user can become a target of a hacker attack.

Commercial organizations do not consider ensuring security as their primary duty, but they have historically treated the expenses for it as inevitable. To some extent, this is a "sensible action": after all, without it, obstacles would overflow even in routine operations. However, have you ever seen the "industrial captains" who dare to allow unrestricted access to all corporate buildings day and night? Certainly not! Even at the entrance to a small company building, you will be met by a security guard or a system that limits and monitors access. Yet, protecting information is still not as effective as desired. Not everyone fully understands how information can be lost and what consequences it may bring.

Computer security is a part of information security that describes the impossibility of damage to a computer, caused by all identified and studied sources of faults, exceeding the amount of harm it can withstand under certain operating conditions and over a specific period of time.

Computer virus — a program that travels through the Internet, destroys computer programs, and causes them to stop working. Today, antivirus programs have been developed to combat these viruses. The earliest mention of viruses appears in the 1977 science fiction work by American T. J. Ryan, which discusses 7,000 computers being infected with a virus. A virus is structured like a program but is harmful. Today, viruses have a wide classification and operate extensively. For example, Kaspersky antivirus could detect 1.5 million viruses (data from 2009). The world's first virus program was placed on the Internet in 1988 by Robert Morris, a graduate student at Cornell University. This virus exploited Unix operating system vulnerabilities for malicious purposes. Robert Morris's virus caused significant damage. Morris himself was sentenced to a long-term imprisonment, but his name remains in history forever.

A computer virus is a dangerous "program" of a computer system. It is installed in the system without the owner’s knowledge and against their will, spreading by attaching to executable files. Computer viruses disrupt normal operations, delete data, distort images on the display, and slow down computational processes. Developers of computer viruses appeared in the early 1980s in the USA and later spread worldwide. Special programs are developed to fight computer viruses.

Most dangerous computer viruses in the world:

1. Morris Worm (1988) – Created by Robert Morris, one of the first harmful programs to spread via the Internet, repeatedly loading itself on computers, causing an estimated $96.5 million in damage.

2. Chernobyl (CIH) (1998) – This virus completely disabled operating systems and erased the Flash BIOS chip, causing irreversible damage to many computers.

3. Melissa (1999) – Spread via email through Microsoft Word documents, automatically sending itself to contacts, disrupting corporate email systems.

4. ILOVEYOU (2000) – Spread via email, destroying personal data and causing significant system damage.

5. Code Red (2001) – Attacked web servers, disabling thousands of websites, causing $2.6 billion in losses.

6. Slammer (2003) – Disrupted Internet networks, causing problems from ATMs to aviation services.

7. Mydoom (2004) – Slowed computers worldwide and caused massive Internet disruption.

8. Conficker (2008) – Infected over 9 million computers and compromised security systems.

9. Stuxnet (2009) – Targeted industrial systems, particularly nuclear facilities.

10. WannaCry (2017) – Attacked computers in over 150 countries, blocked systems, and demanded ransom.

Ways to protect against viruses:

Use reliable antivirus software;

Do not open unknown emails;

Regularly update systems and programs;

Create backup copies;

Be cautious online and avoid suspicious websites.

Malicious software (malware) is any software that disrupts computers, servers, clients, or networks, steals personal data, gains unauthorized access to systems, and prevents users from accessing information. Such software can sometimes be caused by flaws and is generally considered a software defect. Malware causes serious problems for individuals and organizations online. According to Symantec's 2018 Internet Security Threat Report (ISTR), malware increased to 669,947,865 in 2017, twice the 2016 figures. Cybercrime, including malware attacks and other computer crimes, cost the global economy $6 trillion in 2021, increasing at 15% annually.

Types of malware include: viruses, worms, trojans, ransomware, spyware, adware, and destructive programs. Protection strategies vary by type, but often include antivirus software, firewalls, daily threat reduction, network protection, regular backups, and isolation of infected systems. Malware attempts to evade detection by antivirus algorithms.

Computer malware (viruses) is designed to damage systems, steal data, or encrypt files for ransom. Common types include viruses, worms, trojans, spyware, and ransomware.

Key malware types and descriptions:

Viruses: Small programs that hide in other programs, activating when run and damaging files.

Worms: Self-replicating programs that spread through networks.

Trojans: Programs disguised as useful software but harmful to the system.

Ransomware: Encrypts files and demands payment for restoration.

Spyware: Secretly collects personal data, passwords, and online activity.

Rootkits: Hide in deep system areas to evade antivirus detection.

Logic bombs: Activate under specific conditions, e.g., deletion of a certain file.

Computer viruses are one of the most pressing issues today, widely discussed in books and articles. Thousands of professionals work in many companies to combat them. Viruses are a major cause of information loss and have disrupted many organizations and companies. For example, in a hospital in the Netherlands, a patient died due to a computer system error linked to malware.

Virus-infected computers often experience slowed program execution, file size changes, unusual errors, and data or system file loss. Some viruses replicate harmlessly, only displaying incorrect information. However, some are harmful, deleting information on hard drives. Viruses are written maliciously by programmers with intent to harm, often replicating and attaching to executable files.

The virus program aims to disrupt or delete data. The first viruses appeared in the USA, where personal computers were widely used. Initially, they aimed to disturb the user’s peace and nerves, but later intentionally caused damage. Today, over 200,000 viruses exist worldwide. Computer viruses damage data or reduce computer efficiency.

One example is D. N. Lozinskiy, who compared a virus to a clerk: the clerk duplicates papers and passes them to neighbors, causing uncontrolled multiplication. Similarly, a computer virus copies itself to other programs, spreading through the system. If one virus replicates every 30 seconds, it can exceed 1 billion copies in an hour, potentially filling computer memory. The 1988 Morris Virus incident in the USA illustrated this rapid spread through the global network.

How a virus spreads:

1. Virus copies transfer quickly to other programs.

2. Some activate on specific dates, e.g., the "Jerusalem" or "Time" virus deletes files on Friday the 13th.

Computer viruses are replicating programs that transfer to other programs, causing harmful effects. Their detection depends on their replication and integration in the system. Viruses are human-created, unlike biological viruses, and can severely disrupt users’ computers, deleting hard disk data or halting operations. Entry points include diskettes, CD-ROMs, network interfaces, modems, or emails.

Disks are easily infected; inserting an infected disk can place the virus in the boot sector.

Encryption is a cryptographic method using complex algorithms to convert plain text into unreadable ciphertext, which cannot be decrypted without authorization. The process uses cryptographic keys: one key encrypts, and the matching key decrypts. Without the decryption key, the text remains unreadable.

Encryption is an effective method to protect sensitive information but complex to implement and manage. Authorized users can convert ciphertext back into readable text using the correct key. A dual-key system ensures secure communication and storage while protecting against unauthorized access.

How encryption works:

Uses cryptographic keys for encryption and decryption;

Complex algorithms convert plain text into random, unreadable sequences;

Can be symmetric (one key) or asymmetric (public-private key pair)

Reversibility allows authorized access while keeping data secure;

Strong key management is crucial for security.

Today, passwords are essential for computers, websites, forums, emails, and many other services. For trivial sites, any password may suffice, but serious accounts require strong, reliable passwords. Otherwise, malicious actors may access accounts, impersonate users, send messages, or commit financial fraud.

Password cracking often uses brute force, checking all possible combinations. Specialized programs quickly test many variants. Examples:

"09071995" – 1–2 seconds;

"akmal" – 4 seconds;

"Akmal" – 3–4 minutes;

"1n2f4g8y0" – 4 days;

"EC3+gHFBI" – 12 years;

"kKC% maybe million years for finding it.

Computer Security is the protection of computer systems, data, and networks from unauthorized access, theft, and malicious software. With the advancement of information technology today, computer security has become critically important for every user and organization. Viruses, hackers, and malicious software pose significant threats to computer systems and users’ personal information. Viruses can damage files and slow down system performance, hackers can gain unauthorized access to steal data, and malicious software can cause various types of harm to a computer.

To ensure computer security, various methods are employed. Antivirus programs help detect and remove viruses and malicious software, strong passwords and two-factor authentication protect user accounts, and encryption converts data into unreadable form. Users also play a key role in security: avoiding disclosure of personal information online, being cautious of phishing messages, and downloading programs only from trusted sources enhance user security.

As a result, computer security serves as an essential tool for protecting data, ensuring financial and personal safety, and guaranteeing uninterrupted system operation. Therefore, every user and organization must pay serious attention to computer security.

Adabiyotlar, References, Литературы:

1. M.M. Aripov, B.E. To’rayev — Fundamentals of Information Security.
2. S.K. Ganiyev, A.A. Ganiyev — Information Security in Computer Networks.
3. T.X. Xolmatov, N.I. Tayloqov — Informatics and Computing Technology.
4. I.A. Karimov — Information Security.