Проведені дослідження вказують на відповідність розподілу частот відносно голосних звуків, які вносять найбільшу вагу в формування формант в мовному сигналі. Встановлено, що українські голосні звуки "і" та "и", розташовані в частотному діапазоні 200 – 500 Гц, більшість інших голосних звуків лежать в діапазоні від 500 до 1500 Гц. Зважаючи на це, раціональним є окремий розгляд цих частотних діапазонів, при формуванні характерних ознак мовного сигналу, що дозволяє підвищити кількість параметрів, та набирати більшу статистику при визначенні максимумів формантих частот.

Результатом проведеного огляду підходів до визначення формантних частот став алгоритм, що складається з наступних складових:

1. Розділення МС на часові фрагменти.
2. Для кожного фрагменту отримання спектру.
3. Побудова огинаючої лінії.
4. Находження всіх максимумів.
5. Визначення положень формант.
6. Побудова графіків траєкторії положення формант.
7. Розрахунок залежності щільності імовірності розподілу кожної з чотирьох формантих частот (максимумів формантих частот).

Згідно розглянутого підходу до визначення формантних частот необхідно побудувати огинаючу спектру для кожного з фрагментів мовного сигналу. Фактично побудова функції огинаючої представляє собою задачу інтерполяції.

Результатом розрахунку огинальної буде сумісний графік спектру мовного сигналу, в заданому фрагменті, та огинальної спектру для цього ж інтервалу.

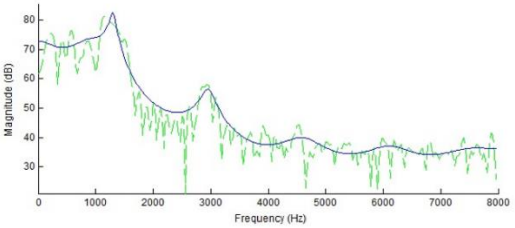

Рис. 2. Огинальна спектру мовного сигналу

Проведений порівняльний аналіз показує достатньо високу точність визначення формантих частот в порівнянні з кепстральним та LPC методами. Поряд з цим, необхідно відзначити простоту реалізації, низьку обчислювальну складність, швидкість та відповідність методу існуючим фізичним процесам.

Information security methods in the enterprise

УДК 316.774:351.75

Svetlana Ermishova, Kurhuzenkova Lyudmila, Husey Qiyasov
European University, qgusein@gmail.com

In order to start listing the methods of protecting information in an enterprise, you need to decide what types of information security threats are often encountered by the enterprises themselves.

- Natural.

These are threats caused by reasons beyond human control. These include hurricanes, fires, lightning strikes, floods, and other natural disasters.

- Artificial.

This is a complex of human-created information security threats. Man-made threats, in turn, are divided into intentional and unintentional. Intentional threats include the actions of competitors, hacker attacks, sabotage of offended employees, etc. Unintentional threats arise as a result of actions committed due to lack of competence or through negligence.

- Internal.

These are threats that arise within the information infrastructure of an enterprise. These include:

1. aging and wear and tear of hardware parts, as a result of which data is damaged;
2. computer resources are used incorrectly;
3. the software is used incorrectly or incorrectly;
4. over time, a large number of various errors accumulate in the data structure, which can lead to their damage.

- External.

These are threats that originate outside the information infrastructure of the enterprise. There are also passive threats and active threats. Passive threats are influencing factors that cannot change the content and structure of information.

Active threats are influencing factors that can change the content and structure of information. These include malicious software. Malware means the following:

1. viruses;
2. macro viruses for Word and Excel;
3. boot viruses;
4. script viruses, including batch viruses that infect the Windows shell, Java applications, etc.
5. keyloggers;
6. programs for stealing passwords.

In order to build competent and professional protection for the enterprise, information security concepts are created. Due to the fact that each enterprise has different areas and volumes of data, different structures, there are individual approaches to the creation of concepts, which take into account all the specifics and characteristics of a particular enterprise. An example of one of the concepts is as follows:

- develop internal documentation that establishes the rules for working with computer equipment and confidential information;
- conduct briefings and periodic checks of personnel; initiate the signing of additional agreements to labor contracts, which indicates responsibility for the disclosure or misuse of information that has become known from work;
- delimit areas of responsibility in order to exclude situations when the most important data sets are at the disposal of one of the employees; organize work in common workflow programs and make sure that critical files are not stored outside network drives;
- implement software products that protect data from copying or destruction by any user, including the top management of the organization;
- make plans for system recovery in case of failure for any reason.

Let's move on to the means of protecting information. What do means of information protection mean? Information security means are devices, devices, gadgets, software, organizational measures that prevent information leakage and ensure its preservation under the influence of the entire spectrum of current threats.

A wide range of specialized software is used to protect data in modern networks. The following types of software protection can be distinguished:

- Antivirus software. Specialized software for detecting, neutralizing and removing computer viruses. Discovery can be performed during scheduled or administrator-run scans. Programs detect and block suspicious program activity in "hot" mode.
- Cloud antiviruses (CloudAV). Combining the capabilities of modern antivirus programs with cloud technologies. Such solutions include Crowdstrike services, Panda Cloud Antivirus, Immunet and many others. All the basic functionality of the software is located in the cloud, and a client is installed on the protected computer - a program with minimal technical requirements. The client uploads the bulk of the data analysis to the cloud server. This ensures effective anti-virus protection with minimal resource requirements for equipment. CloudAV solutions are ideal for protecting PCs that do not have enough free computing power to run standard antivirus.
- DLP (Data Leak Prevention) solutions. Special software solutions to prevent data leakage. This is a set of technologies that effectively protect enterprises from the loss of confidential information for a variety of reasons. Implementation and support of DLP - requires a fairly large investment and effort on the part of the enterprise. However, this measure can significantly reduce the level of information risks for the company's IT infrastructure.
- Cryptography systems. They transform the data, after which their decryption can only be performed using the appropriate ciphers. In addition, cryptography can use other useful applications to protect information, including message digests, authentication methods, encrypted network communications, and digital signatures. Today, new applications that use encrypted communications, such as Secure Shell (SSH), are gradually replacing outdated solutions that do not provide the required level of security in today's environment, such as Telnet and the FTP file transfer protocol. Modern WPA /

WPA2 protocols are widely used for wireless encryption. The rather old WEP protocol is also used, which is inferior in terms of security.

- Firewalls (ITU). Solutions that filter and block unwanted traffic control network access. There are such types of firewalls as network and host servers. Network firewalls are located on LAN gateway PCs, WANs and intranets. The firewall can be executed in the format of a program installed on a regular computer or have a software and hardware implementation.
- Virtual private networks VPN (Virtual Private Network). A solution that uses a private network to send and receive data over a public network, effectively protecting network-connected applications. VPN provides the ability to remotely connect to a local network, creating a common network for the head office with branches. Directly for users, VPN provides location hiding and protection of online activities.
- Proxy server. Serves as a gateway between a computer and an external server. A request sent by a user to the server first goes to the proxy and on its behalf goes to the server. The response is also returned with the passage of an intermediate link - proxy. The advantage is that the proxy server cache is available to all users. This improves usability because the most frequently requested resources are in the cache.
- SIEM solutions - information security monitoring and management systems. Specialized software that takes over the data security management function. SIEM collects information about events from all sources that support security, including antivirus software, IPS, firewalls, as well as operating systems, etc. SIEM also analyzes the collected data and provides its centralized storage in the event log. Based on data analysis, the system identifies possible failures, hacker attacks, other deviations and possible information threats.

Cryptanalysis of Markov ciphers and Markov-type ciphers

УДК 621.395.7 (043.2)

Ruslan Skuratovskii[1], Lisa Kostina[2]
National Aviation University
[1] r.skuratovskii@kpi.ua, ruslan@imath.kiev.ua,
[2] 6324462@stud.nau.edu.ua

The object of the research is block ciphers with a round function of the form $G_k(x) = L_m(S(x \oplus k_i))$ These ciphers are considered from the point of view of their belonging to the class of Markov or generalized Markov cipher.

The main results described in this article are as follows (note that by complexity we mean the number of encryptions required to create all the necessary pairs, and during the attack, the algorithm itself uses, generally speaking, less material). DES with 6 rounds was cracked in less than 0.3 seconds on a personal computer using 240 ciphertext. 8-round DES was cracked in less than two minutes on a computer by analyzing 15,000 ciphertext, selected from a set of 50,000 ciphertext candidates. 15-round DES breaks faster than brute-force, but 16-round DES still requires 2^{58} steps (this is slightly more than brute force complexity).

It is well known, for the DES algorithm, after finding 48 bits of the key of the last round, the remaining 8 bits are complete search [7].