IJARST
International Journal For Advanced Research In Science & Technology
A peer reviewed international journal www.ijarst.in
ISSN: 2457-0362

NETWORK INFORMATION SECURITY TOOLS

[1]Beknazarova Saida Safibullayevna, [2]Absamitov Bekhruz
[1,2]Tashkent University of Information Technologies named after Muhammad Al- Khwarizmi,
105, A. Temur, Tashkent, 100142,Uzbekistan,saida.beknazarova@gmail.com

The protection of information in information networks has become relevant with the development of the Internet. Gadgets transmit data with and without the user's participation. With the informatization of society, more and more attention is paid to the protection of personal data and countering cyber-attacks [1].

In general, it is possible to get into the enterprise network only by having the username and password of one of the users, i.e. by going through the authentication procedure. When transmitting information via the Internet, it is possible to intercept the user name and password. Technically, the issue can be solved by conducting additional authentication of client machines, a two-factor authorization system, and using encryption. Organizing and conducting an audit of events [2].

Wireless network protection

With the development of wireless technologies and their availability, a Wi-Fi router appeared in every home and office. But any convenience carries certain risks. Today, scanners (sniffer analyzers) of wi–fi networks have become available on the market, which can receive password data installed on your wireless device. How to protect yourself from a burglar?

Use a secure password. The password requirements are set out below.

Update the router software regularly. Invite a specialist for these purposes. Perform this procedure at least once a year.

Be sure to write down the password to your device that the master equipment adjuster has set for you.

The WPA network encryption format must be installed In the near future, the WPA 3 encryption standard will appear.

Software tools for protecting information on the network

One of the ways fraudsters get a login and password to access the corporate network is the selection method. To begin with, an attacker may need to get login options, and this can be done by collecting email accounts – from websites, social networks and other profiles of decision makers (LPR). Sometimes LPR use several email accounts, not just corporate ones. Having thus gained access to personal mail, you can try to get access to the corporate one already (for example, by requesting a password to restore it). How to resist this?

Most of the largest email services and social networks offer two-factor authorization - the essence of which is the initial password entry, at the second step, the service authorization system asks you to enter either a one-time code or a code from special programs such as Google Authenticator or Microsoft Authenticator [3].

Authenticator programs are usually installed on a mobile phone and require an Internet connection. In real time, the Authenticator program generates one-time codes that are required to be entered at the second stage of user authorization.

Organizational methods of data protection

If you have used your accounts on corporate devices or in an Internet cafe - do not be lazy - click the "Log out" button and clear your data in the browser. Do not check the "Remember" your account details in the browser.

Personal data protection is also required in the largest services for the sale of personal items such as avito.ru , youla.ru - these services have learned to rank the goods sold according to different criteria, which include cost. To protect the phone number when placing ads in the cars category, the services offer to replace the actual specified number with a virtual one and all calls are forwarded.

Methods of protection:

- Creating obstacles to entry, for example, physical restrictions on access;
- Work on strengthening security elements and vulnerability management;
- Masking of information, including by means of cryptography;
- Regulation of the access level, use of approved protocols;
- Coercive and incentive measures, using administrative, criminal, material liability, as well as moral and ethical rules.

Cryptographic protection is the most reliable way to transmit information via Internet channels. For local and corporate networks, they use:

- authentication via login-password, EDS, etc.;
- regulation of powers, access levels, registration of requests, restrictive measures for unauthorized access.

Means of protection

Technical:

- physical, creating immediate obstacles (locks, doors);
- hardware embedded in the IC to create obstacles and encrypt data;
- software implemented as specialized software with distribution of access levels and encryption;
- legislative, creating standards, defining legal instruments of use and levels of responsibility.

Organizational, limiting and controlling:

- publication of personal content in social networks;
- use of non-corporate (during working hours) and corporate accounts (for personal purposes);
- access to personal information of outsiders;
- information about line personnel on badges;
- the shelf life of paper media and regulating their destruction;
- publishing information about employees in open sources.

Protection technologies

Encryption. The level of protection depends on the complexity of the algorithm. Simple protection of unclassified information – EDS (warns about changes in the original document).

Network tools. Using authentication, two-factor authorization, encryption, and event auditing. To protect wireless networks vulnerable to sniffers, it is necessary to use a strong password, regularly update the router software, know the WI-FI password of the device, use the WPA 3/WPA encryption format.

Software tools. Two-factor authentication via a password–code bundle (one-time or generated in Microsoft Authenticator, Google Authenticator programs).

Protection of information on a PC (laptop)

Viruses, Trojans, spyware and ransomware can steal personal data. To protect yourself from them, you need to:

Use licensed software, updating it regularly.

Regularly check your PC with an antivirus.

Do not work in the "Administrator" mode, always use a user account with limited rights.

Make backups, for example, on cloud services.

Be careful when surfing, so as not to end up on a phishing site.

Do not use the password storage service.

When creating a password, you need to come up with something original using letters, symbols and numbers. Passwords should be changed regularly, without using the same combination on different services.

Create an additional account for authorization on the Internet, used only for this purpose.

Reference:

1. Gafner, V.V. Information security: A textbook / V.V. Gafner. - Ph/D: Phoenix, 2017— - 324 p.

2. Gromov, Yu.Yu. Information security and information protection: Textbook / Yu.Yu. Gromov, V.O. Drachev, O.G. Ivanova. - St. Oskol: TNT, 2017. - 384 p.

3. Efimova, L.L. Information security of children. Russian and foreign experience: Monograph / L.L. Efimova, S.A. Kocherga. - M.: UNITY-DANA, 2016— - 239 p.