UDC 378.16

DATA PROTECTION FROM NETWORK ATTACKS

G. Zhangisina, D. of Engineering, ***E. Kuldeev, A. Shaikhanova***

Kazakh National Technical University named after K. I. Satpayev, Almaty

gul_zhd@mail.ru

Due to the widespread dissemination of informational distributed computing networks reveals problems in information protection from unauthorized access. This article deals with the security problem of informational computer networks from network informational attacks. Revealed in the article stages of unauthorized access to computing informational network, showed that even the protected computing system acquires certain vulnerability when it is connected to the public network. Have been described the characteristics of protection against network attacks. The proposed specifications are of good quality and are expressed requirements to ensure the resistance of certain offender actions. The proposed model of offender actions gives more accurately determine the list of threats, which must be taken into account in the designing of data protection and in security policy of an informational computing network. Considered characteristics give possibility to assess security of the distributed informational computing networks, which consist of geographically dispersed components of various network informational attacks.

Keywords: DAN (data-area networks), information security, network attack, the offender, the characteristics of security, unauthorized access.

У зв'язку з поширенням розподілених інформаційних обчислювальних мереж виявляються проблеми в захисті інформації від несанкціонованого доступу. У цій статті розглянуто проблему захищеності інформаційних обчислювальних мереж від мережевих інформаційних атак. Розкрито етапи несанкціонованого доступу до інформаційної обчислювальної мережі, які показують, що навіть захищена обчислювальна система набуває деякої вразливості під час її підключення до мережі загального користування. Описано характеристики захищеності від мережевих атак. Запропоновані характеристики є якісними і виражаються вимогами щодо забезпечення опору певних дій порушника. Запропонована модель дій порушника надає можливості більш точно визначити перелік загроз, які слід взяти до уваги при розробці системи захисту інформації та політики безпеки інформаційної обчислювальної мережі. Розглянуті характеристики дозволяють оцінювати захищеність розподілених інформаційних обчислювальних мереж, які складаються з територіально рознесених компонентів, від різного роду мережевих інформаційних атак.

Ключові слова: ІОМ (інформаційні обчислювальні мережі), захист інформації, мережеві атаки, порушник, характеристики захищеності, несанкціонований доступ.

Introduction

In today's world are becoming increasingly important information distributed computing networks (DAN). It should be noted that the creation of one of their main tasks is to protect the information from unauthorized access. Unauthorised access, performed by the offender remote access will be called network attack. In order not to have been locked in a timely manner of its action, the offender tends to have information on the actual use network infrastructure, subject to the applicable network technology, network and transport protocols, network services and business applications. If successful, an attacker may be arranged hidden data channel, through which he has a chance to access hosts on the DAN [1].

Stages of unauthorized access

The probability of such a development is caused by three main assumptions [2]:

- availability of transport between hosts DAN;
- the presence of vulnerabilities in the DAN (design errors and / or marketing);
- the presence of a compromise price / performance in the application of information security.

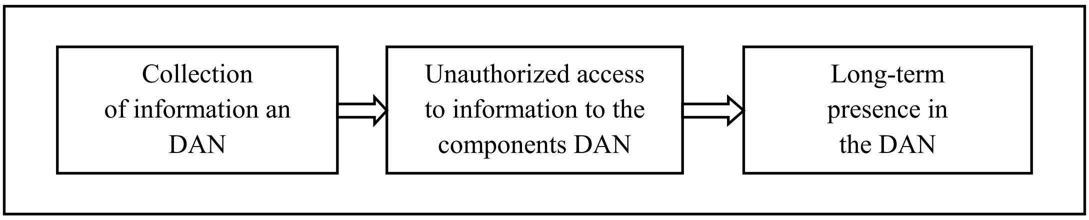

Collection of information an DAN
Unauthorized access to information to the components DAN
Long-term presence in the DAN

Fig. 1. Model of violator

The offender acts in stages (Fig. 1).

© G. Zhangisina, E. Kuldeev, A. Shaikhanova, 2013

Stage I. At the initial stage of a criminal is collected general information about DAN and collect information on potentially sensitive resources. Information of interest to the attacker offered conditionally divided into technical and personal. The first group includes the following data:

- Information about the network and its topology;
- Information about the hosts DAN, including hardware, operating systems, types used, applications, network services provided, etc.;
- Information about security (firewalls, filters, intrusion detection systems).

In addition, the accumulated information of a personal nature on administrators and users of the DAN, allowing to establish the degree of correspondence between the users of the DAN and specific individuals.

Stage II. Once the information is collected about the detention center, over an active attempts breach of security detention center at both the host and the entire system. The purpose of this phase is to implement the threat of violation of confidentiality, integrity and availability of information in the detention center.

Stage III. At this stage, the offender made in the implementation of the DAN funds hidden management, monitoring and correction of internal audit data (programs such as “Trojan horse”). Modification of audit logs helps tamper go unnoticed for the security administrator and systems analysis. Funds hidden controls allow unauthorized access in the future to produce without getting information about the fact of access to audit logs. In addition, these funds is access to resources DAN, which makes the detection of an intruder, and the fact of unauthorized access. After the successful implementation of phase III can be assumed that the offender failed to compromise this host DAN.

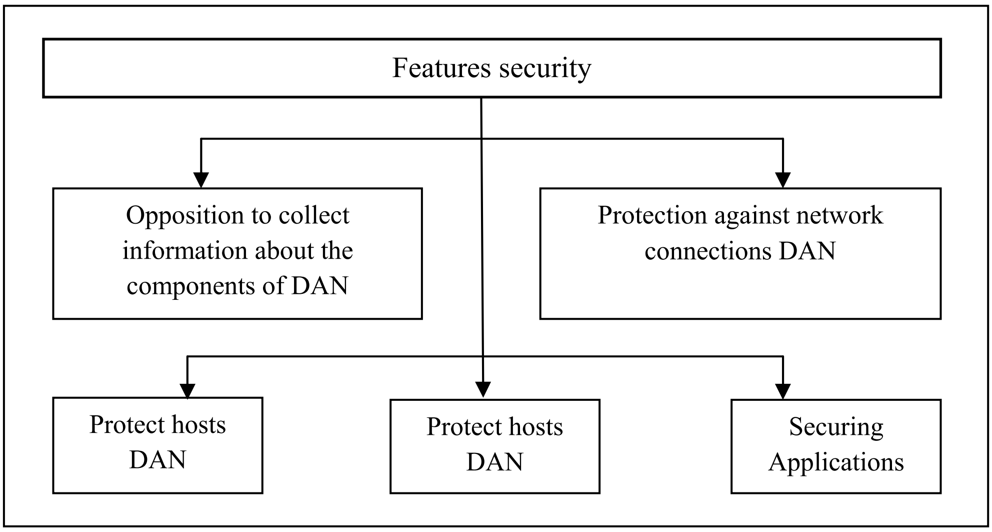
The problem of estimation of security detention center on network information attacks (for example, when you connect to the Internet DAN) is that even the protected computer system acquires a certain vulnerability when it is connected to the public network. This is due to the peculiarities accepted for exchange in the public network communication protocols, communications equipment, rules, information exchange, etc. [3].

Certain protocols and data transfer technologies used in public networks have design flaws and implementation, which lead to a decrease in security detention center. Therefore, to make reasonable efforts to achieve the required level of security is necessary to introduce new security features that will be given in the form of requirements. The proposed specifications are of good quality and are expressed requirements to ensure the resistance of certain actions offender.

Features security

We divide conditionally all indicators into five groups (Fig. 2) [4].

The first group includes performance counter collection of information about the components of the DAN.


Features security
Opposition to collect information about the components of DAN
Protection against network connections DAN
Protect hosts DAN
Protect hosts DAN
Securing Applications

From opposition to the establishment of IST (information security tools) is required:

- the type of operating systems;
- hardware platform component DAN;
- the availability of network services;
- versions of software tools;
- active hosts.

IST should also prevent the possibility of studying the topology of the network and obtain information about users of the DAN.

The second group comprises security characteristics of network connections DAN.

IST prevents:

- the possibility of “listening” segment;

- uncontrolled transfer of network packets between interfaces, one host;
- Organization of unauthorized access to communication channels DAN;
- the possibility of unauthorized network devices are connected.

The third group of indicators relates to the safety of hosts DAN. It will include features such protection as fighting capabilities:

- uncontrolled access to system files and change them;
- interception and modification of audit records;
- exhaustion of system resources processes;
- reducing the secrecy when dealing with objects;
- the appearance of the operating system components that are not needed for functionality within the tasks performed;
- the occurrence of inappropriate access privileges to critical system files.

The fourth group describes the characteristics of network security detention center. The protection system must withstand:

- attacks such as “denial of service” at the network level;
- “spoofing”, ie attacks on the authentication mechanisms that are based on sender address verification;
- transmission of passwords in clear text;
- transmission of data with limited access to unencrypted;
- the use of network protocols with weak authentication;
- violation of the integrity of transmitted data;
- use of alternative security mechanisms that lower the level of protection;
- the availability of protocols that are not needed for the work of the tasks performed.

And finally, the fifth group describes the characteristics of application security. The system should not miss:

- inadequate access permissions for files;
- application components that are not needed for the work of the tasks performed;
- Anonymous access to the application's resources.

IST should also prevent the possibility of modifying records application logs.

Conclusion

The proposed model provides the violator's ability to accurately identify a list of threats that must be taken into account in the development of IST and security policy DAN.

The above characteristics make it possible to evaluate the distributed security detention center, which consist of geographically dispersed components of various network information attacks.

REFERENCES

1. *Shangin V.* Protection of information in computer systems and networks/ V. Shangin. — DMK-Press, 2012. — 592 p.

2. *Domarev V.* Safety of information technology. The systems approach. / V. Domarev — K. : TID Dia Software Ltd., 2004. — 992 With.

3. *Zegzhda D.* Fundamentals of Information Systems Security / D. Zegzhda, A. M. Ivashko. — Moscow Hotline-Telecom, 2000. — 452 pp.

4. *Smoked A.* Information security audit / A. Smoked, S. Zefirov, V. Golovanov. — BDC-press, 2006. — 304.

5. *Stoling William*. Cryptography and network security: Principles and Practice, 2nd ed.: Trans. from English / William Stoling. — M. : Publishing house “Williams”, 2001. — 672 s.

6. *Torokina A.* Engineering and technical protection of information / A. Torokina. — Publisher “Helios ART”, 2005. — 960.

Article received 11.03.13.