**УДК 004.056.53:004.492.3 (045)**

***Гизун А.И., Волянская В.В., Гнатюк В.А. Модели эталонов лингвистических переменных для систем обнаружения и идентификации нарушителя информационной безопасности***
***Аннотация.*** *Изучение факта нарушения информационной безопасности и личности нарушителя имеет большое научное и практическое значение. С этих позиций, формализация параметров, которые могут быть использованы для идентификации нарушителей, является актуальной научной задачей. Четкое определение полного множества параметров позволит повысить эффективность превентивных мер и систем защиты. В работе предложена модель эталонов лингвистических переменных, ориентированная на построение системы обнаружения нарушителя (вторжение). Для обнаружения нарушителя используется ряд хостовых и сетевых параметров, большинство из которых имеют нечеткую природу. На основе проведенного эксперимента построены модели эталонов этих параметров с использованием нечетких чисел. Полученные результаты могут быть базисом для построения системы обнаружения вторжений на основе технологии honeypot.*
***Ключевые слова:*** *нарушитель информационной безопасности, система обнаружения нарушителя, параметры, идентификация, лингвистические переменные, нечеткая логика, эталоны параметров.*

***Gizun A.I., Volyanska V.V., Gnatyuk V.O. Etalon models of linguistic variables for information security intruders' detection and identification***
***Abstract.*** *Study of information security breach and intruder identity has a great scientific and practical importance. From this viewpoint parameters formalization for intrude identification is an actual research problem. Clearly definition of complete set parameters can give a possibility to increase preventive measures and security systems efficiency. In the paper etalon model of linguistic variables was proposed and oriented on IDS system construction. For intruder detection the set of host and network parameters are used. Most of them have a fuzzy nature. The etalon models were build using fuzzy numbers on basis of experiment. Given results can be the basis for IDS system based on honeypot-technology development.*
***Key words:*** *information security intruder, intruder detection system, parameters, identification, linguistic variables, fuzzy logic, etalon parameters.*

Отримано 23 *січня 2012 року*, затверджено редколегією 27 *лютого 2013 року*

# DATA PROTECTION FROM NETWORK ATTACKS

**Gulnur Zhangissina, Erjan Kuldeev, Ajgul Shayhanova**

*Kazakh National Technical University named after K.I.Satpayev, Kazakhstan*

**ZHANGISSINA Gulnur D.**, Doctor of Science (DSc), Professor

*Date and place of birth:* 1958, Almaty, Kazakhstan.
*Education:* Kazakh National University named after Al-Farabi, 1980.
*Research interests:* information security, computer security, parallel computing, information systems and distance education.
*Current position & Functions:* Head of the Computer Science Department.
*Publications:* more than 200 publications, including 4 monographs, over 20 books & 180 papers.
*E-mail:* gul_zhd@mail.ru

**KULDEEV Erjan I.**, PhD, Professor

*Date and place of birth:* 1973, Aralsk, Kyzyl-Orda region.
*Education:* Geological Department of the Kazakh Polytechnic Institute named after Lenin, in "Geophysical methods of exploration" for qualified mining engineer-geophysicist.
*Research interests:* information security, computer security, GIS.
*Current position & Functions:* Vice Rector for science and innovation.
*E-mail:* kuldeev@ntu.kz

**SHAIKHANOVA Ajgul K.**

*Education:* GU "Semey", 1998, KazFEA, 2011
*Research interests:* information security, computer security, parallel computing, information systems.
*Current position & Functions:* PhD student.
*Publications:* more than 30 publications, 8 e-books.
*E-mail:* igul7@mail.ru

***Abstract.*** *This article describes the steps of unauthorized access to the informational computing network. Proposedaction model is providing a violator to more accurately determine the list of threats that must be taken into account in the development of data protection and security policy of informational computing network.*

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

### 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.

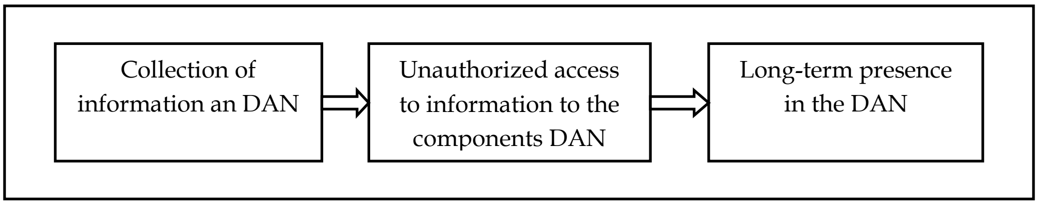

Collection of information an DAN
Unauthorized access to information to the components DAN
Long-term presence in the DAN

Fig. 1 Model of violator

The offender acts in stages (Fig. 1).

*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.

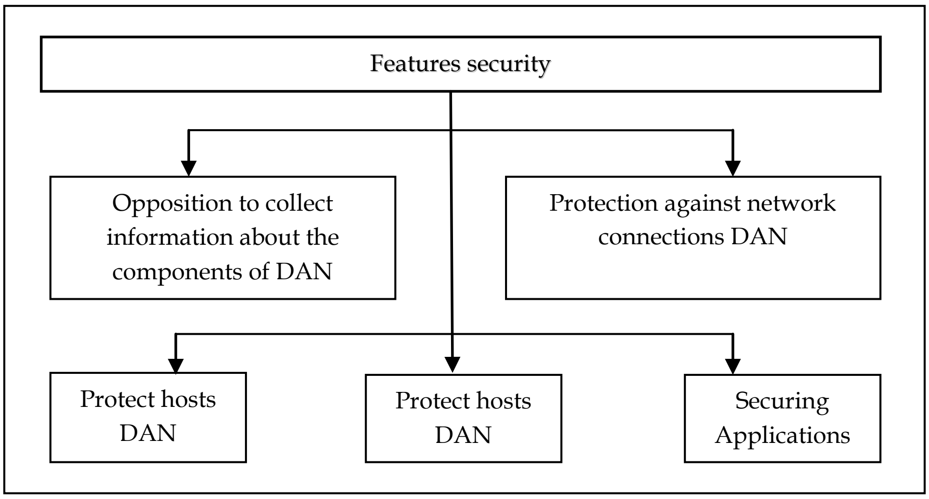

Features security
Opposition to collect information about the components of DAN
Protection against network connections DAN
Protect hosts DAN
Protect hosts DAN
Securing Applications

Fig. 2. Proposed features protection from network attacks

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.G. Protection of information in computer systems and networks. - DMK-Press, 2012, 592 p.

[2] Domarev V.V. Safety of information technology. The systems approach. / V. Domarev - K.: TID Dia Software Ltd., 2004. - 992 p.

[3] Zegzhda D.P. Fundamentals of Information Systems Security / DP Zegzhda, A.M.Ivashko - Moscow Hotline - Telecom, 2000. 452 p.

[4] Smoked A.P. , Zefirov S.L. , Golovanov V.B. Information security audit. - BDC-press, 2006. – 304 p.

[5] Stoling William. Cryptography and network security: Principles and Practice, 2nd ed.: Trans. from English. -M.: Publishing house "Williams", 2001. – 672 p.

[6] Torokina A.A. Engineering and technical protection of information. Publisher "Helios ART", 2005. – 960 p.

**UDC 378.16 (045)**

***Жангісіна Г.Д., Кульдеев Є.І., Шайханова А.К. Захист даних від мережевих атак***
***Анотація.*** *У даній статті розглянуті етапи несанкціонованого доступу до інформаційної обчислювальної мережі. Запропоновано модель дій порушника, що дасть можливість більш точно визначити перелік загроз, які слід взяти до уваги при розробці системи захисту інформації та політики безпеки інформаційної обчислювальної мережі.*
***Ключові слова:*** *ІОМ (інформаційні обчислювальні мережі), захист інформації, мережеві атаки, порушник, характеристики захищеності, несанкціонований доступ.*

***Жангисина Г.Д., Кульдеев Е.И., Шайханова А.К. Защита данных от сетевых атак***
***Аннотация.*** *В данной статье рассмотрены этапы несанкционированного доступа к информационной вычислительной сети. Предложена модель действий нарушителя, предоставляющая возможность более точно определить перечень угроз, которые следует принять во внимание при разработке системы защиты информации и политики безопасности информационной вычислительной сети.*
***Ключевые слова:*** *ИВС (информационные вычислительные сети), защита информации, сетевые атаки, нарушитель, характеристики защищенности, несанкционированный доступ.*

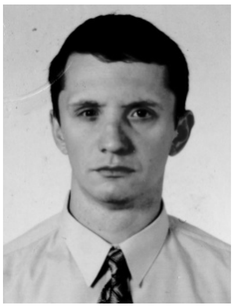
Отримано *25 січня 2013 року*, затверджено редколегією *1 березня 2013 року*

# ЗАХИСТ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ТА ОБЛАДНАННЯ / SOFTWARE & HARDWARE ARCHITECTURE SECURITY

# НЕЙРОМЕРЕЖЕВА МЕТОДОЛОГІЯ РОЗПІЗНАВАННЯ ІНТЕРНЕТ-ОРІЄНТОВАНОГО ШКІДЛИВОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

**Ігор Терейковський**

*Національний технічний університет України «Київський політехнічний інститут», Україна*



**ТЕРЕЙКОВСЬКИЙ Ігор Анатолійович,** к.т.н., доцент

*Рік та місце народження:* 1967 рік, м. Тернопіль, Україна.
*Освіта:* Київський інститут інженерів цивільної авіації (з 2000 року – Національний авіаційний університет), 1992 рік.
*Посада:* доцент кафедри системного програмування та спеціалізованих комп'ютерних систем з 2009 року.
*Наукові інтереси:* інформаційна безпека.
*Публікації:* більше 50 наукових публікацій, серед яких монографія, навчальні посібники та наукові статті.
*E-mail:* terejkowski@ukr.net