УДК 681.3.06
DOI: 10.18372/2310-5461.34.11608

B. Y. Korniyenko — Dr. habil., associate professor
National Aviation University
e-mail: bogdanko@i.ua
orcid.org/0000-0002-2521-0878

L. P. Galata
National Aviation University
e-mail: galataliliya@gmail.com
orcid.org/0000-0002-7978-3954

DESIGN AND RESEARCH OF MATHEMATICAL MODEL FOR INFORMATION SECURITY SYSTEM IN COMPUTER NETWORK

Introduction

Efficient construction and usage of corporate information systems has become an extremely important task, especially in insufficient funding of information technology in enterprises. Evaluation criteria for efficiency are the cost reducing of the information system implementation, current and nearest future requirements compliance, the opportunity and the cost of further development and transition to new technologies [1–3].

The information system core is a computing system that includes next components: cable network and active network equipment, computer and peripheral equipment, data storages (libraries), system software (operating systems, database management systems), special software (monitoring and network management) and in some cases the applied software [4–7].

Task formulation

The purpose of research is to construct and study mathematical model for Information Security System in Computer Network by using modern software.

The main material

Now the most common approach in information systems design is to use expert estimates. According to this approach, experts in the field of computing tools, active network equipment, cable networks, design computing system to solve the specific task or class of tasks, based on their experience and expert estimates. This approach minimizes the cost of the design stage, quickly estimate the cost of implementing the information system. However, decisions obtained by using expert estimates are subjective, hardware and software requirements as the assessment of guarantees for efficiency of proposed system project are subjective too.

As an alternative may be used approach, which involves the development of models and modeling (simulation work - simulation) of computing system behavior. The modeling is a fundamental method for studying the behavior of complex systems.

The modeling is one of the main methods of knowledge, and a form of reflection of reality. The modeling is to clarify or reproduction of certain properties of real objects, things and events through other objects, processes, events, or through abstract descriptions such as image, plan, map, set of equations, algorithms and applications.

The model is defined as "a system that is provided or material implemented, that is replaced the real object (system) in the process of cognition or analyzing, while retaining some of the most important features for its research, and its study gives us new information about the object.

Here are the main types of models used in practice to describe the different processes and systems:

- the conceptual model — the model describes the system using special characters, symbols, operations or using natural or artificial languages;
- the physical model — the system reproduces based on the ratio of similarity, that is resulting from the similarity of physical phenomena;
- the structural and functional model — as a model uses scheme (block diagram), tables, graphs, diagrams and drawings with special rules of their union and transformation;

- the math model is a math representation of reality, the description of some phenomenon or system using math concepts and symbols;
- the simulation model — economic and math model uses in the experimental study of system or phenomena by using personal computers.

These types of models can be used both individually and a few at a time, also, when you use simulation modeling, it involves all of these types or their separate techniques. The simulation model allows us to visualize the final or intermediate result dynamically, that is an important aspect for a successful understanding the received results by persons who did not participate in its development.

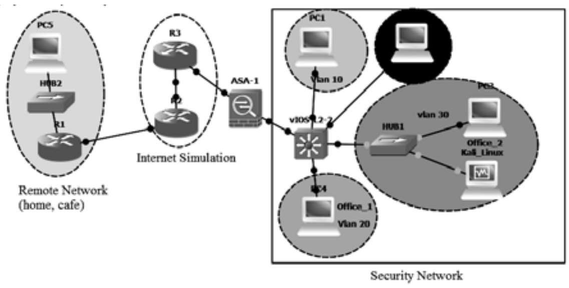
Common definitions of term "simulation modeling":

- it is the method allows to build models that describe the processes as they would take place in reality. Such model can be "plaied" for a single test or set of tests. The results will be determined by the random behavior of the process;
- it is the research method in which studied system is replaced by a model that accuracy describes the real system, with which experiments are conducted to obtain information about this system;
- it is the special case of math modeling. There is a class of objects, for which have not developed analytical models or solution methods of resulting model for various reasons. In this case, the analytical model is by the simulator or simulation model;
- it is logical and mathematical description of an object that can be used to experiment on your computer in order to design, analysis and assessment of the object.

Simulation modeling is used to study the behavior of the system by using math tools and computing equipment. The calculation of the required results may be automated by using computing technology, with only initial data, for example, been obtained statistically. It is especially important, when complex system that consist of many components is being used, because for calculation of required results you need to use cumbersome formulas usually. Simulation modeling is applied to study the behavior of various systems, including the information one [1], [2].

Mainly in information systems modeling there is an aim to achieve information about request processing time or resource load level. As for computing networks, their simulation models reproduce the processes of message generation by applications, of splitting messages into specific protocols packets and frames, of delays in processing messages, packets and frames within the operating system, of computer access to the shared network environment, of router incoming packets processing and etc. No need to buy expensive equipment by using simulation modeling network - its work simulates by programs that accurately reproduce such equipment main features and options.

It was offered to use simulation modeling for determination the actual security threats [3]. GNS3 Cisco Systems software have been selected as the simulation environment (see figure).



The simulation model of information security system in computer network

The choice of this software due to the following factors:

- a process of creating models is facilitated by using a graphical development environment;
- previously created modules and libraries can be used to create new models;
- object-oriented approach to model building;
- a large number of built-in libraries for creating simulation models;
- models can be run at any software and hardware platform;
- a simulation model can be run without development tools.

Graphical Network Simulator GNS3 is a cross-platform program with open source. It is based on popular Dynamips (CISCO IOS emulator), Dynagen (Dynamips text interface) and Pemu (Cisco PIX emulator).

GNS3 provides easy to use GUI, and a range of other features. You can model the new configuration, various images of IOS, or perhaps, make fully reconstruction of some complex network parts. That is much easier with this program than its be in a real network. The product processes the installation and configuration of essential utilities automatically. The GNS3 installation package includes all emulators. In the case of GNS3 installation on the Microsoft Windows operating system, you must also install WireShark, it is necessary to intercept monitor network packets and libraries.

Sometimes, it is not enough network devices in the company and there is no router, which deals with internal networks routing, but there is only

L2-switch and security device Cisco ASA with IOS 8.4.2 version. So, it is necessary to set additional functionality on Cisco ASA, such as routing. Similarly, we have only one interface to connect with the L2-switch. Also we need to configure remote users' connections by VPN.

There is the next task: the networking between internal networks should be organize to meet the requirements of security. The guest network access should be organize only to "INTERNET" with limited speed of 1024 Kb. The remote users connect should be organize through Remote Access VPN, therefore remote users should connect to the internet via Cisco ASA device and have access to the internal resources of the company. Internal website should be available on "INTERNET". All of this tasks should be done through CLI. We have a central office with installed Cisco ASA device and L2-switch. Four networks (VLANs) have been created at switch, which submitted to security device through Trunk.

There are the characteristics of each VLAN-s:

- Vlan_Office_1 — network 192.168.2.0/24.

Security Level is 100. It is uses for first part of employees. There are the Internet access from this subnet, and Vlan_Office_2, Vlan_DMZ and Vlan_Guests access;

- Vlan_Office_2 — network 192.168.3.0/24.

Security Level is 100. It is uses for second part of employees. There are the Internet access from this subnet, and Vlan_Office_1, Vlan_DMZ and Vlan_Guests access;

- Vlan_DMZ — network 192.168.1.0/24.

Security Level is 50. There is a Web-Server (WWW-SRV) with company's website in this network. Accordingly, it is available from Internet at port 80 (TCP) and there are access from Vlan_Office_1, Vlan_Office_2 subnets to this network and from Vlan_Guests subnet at 80th port;

- Vlan_Guests — Guest subnet 192.168.4.0/24.

It is uses for "guests" who came to our office. Security Level is 10. There are the Internet access from this subnet with limit speed of 512 Kb and access to the internal website (SRV-WWW) only at 80th port.

There is a network, that simulates "INTERNET", which uses two routers (Router_1 and Router_2). There is loopback-interface (IP-address 1.1.1.1) at Router_1, which will be use to check for the "INTERNET". Dynamic routing protocol OSPF is used for routes exchange. Also there is a remote user, which is placed in the subnet 192.168.5.0/24 (say it is internet-cafe) behind Remote_Router. This remote user has access to the Internet but he is considered dangerous without VPN connection to the central office.

A simulation model consists of protected and unprotected networks. The main element of information security system is the firewall ASA 8.4, a platform for atak- set Kali Linux. Kali Linux is modern Linux-distribution for penetration testing and security audit. Kali is a complete reassembly BackTrack Linux, fully according to Debian development standards.

All new infrastructure has been revised, all the tools were analyzed and packaged, and we switched to Git for our VCS.

- There are more than 300 tools for penetration testing: After considering each tool that was included in BackTrack, we have removed a large number of tools that either do not work or duplicate other tools with similar functionality.
- Kali Linux is completely free and always will be free. You will never have to pay for Kali Linux.
- Git tree with open source code: our tree is open to all, and all of sources available for set up or rebuild packages.
- FHS compliant: Kali was designed to observe the Filesystem Hierarchy Standard, which allows all Linux users easily find executable files, support files, libraries, etc.
- Wide support for wireless devices: Kali Linux was built to support many wireless devices, allowing it to work correctly with a wide range of hardware devices and making it compatible with many USB and other wireless devices.
- Special core patches from injection: developers often need to audit wireless networks, so our core includes the latest patches for them.
- Secure Development Environment: Kali Linux development team consists of a small group of trusted persons who can add packages or interact with storage only by using several secure protocols.
- GPG signed packages and repositories: All packages are signed by each individual Kali developer when they are created and recorded, and then the repository signed packages also.
- Multilingual: Kali has a true multi-language support, allowing most users to work in their native language and to find the tools needed for the job.
- Customizable: You can as easy as possible customize Kali Linux to your taste, down to the core.
- Support ARMEL and ARMHF: Kali supports ARM-systems and has installations for ARMEL and ARMHF systems. Kali Linux ARM repository is integrated with the main distribution.

LOIC was used to implement attacks. The program performs a distributed attack such as "denial of service" by TCP-, UDP-packets or HTTP-requests regular transfer to the certain site or host with a goal to destroy the target node. There is also an edition of the program LOIC Hive Mind, that automatically receive the task to attack via IRC, RSS or Twitter, which allows centralized DDoS-attacks.

Attacks occur from a remote location to internal subnet (Office_1, Office_2, DMZ, Guests) with different security levels. There are customized security levels: offices — security level is 100, the traffic between offices is not filtered. DMZ security level — 50, Guests-10. Offices trafik is unrestricted with other subnets, there is access from DMZ to Guest subnet, there is access from the guest subnet only to the Internet. Internet working is emulated by two routers with loopback-interface.

Conclusions

Using modeling in the design of computing systems, you can:

- estimate the bandwidth of the network and its components;
- identify vulnerability in the structure of computing system;
- compare different organizations of a computing system;
- make a perspective development forecast for computering system;
- predict future requirements for network bandwidth;
- estimate the performance and the required number of servers in the network;
- compare various options for computing system upgrading;
- estimate the impact of software upgrades, workstations or servers power, network protocols changes on the computing system.

Research computing system parameters with different characteristics of the individual components allows us to select the network and computing equipment, taking into account its performance, quality of service, reliability and cost. As the cost of a single port in active network equipment can vary depends on the manufacturer's equipment, technology used, reliability, manageability.

The modeling can minimize the cost of equipment for the computing system. The modeling becomes effective when the number of workstations are 50–100, and when it more than 300, the total savings could reach 30–40 % of project cost.

REFERENCES

1. **Корнієнко Б. Я.** Дослідження моделі взаємодії відкритих систем з погляду інформаційної безпеки / Б. Я. Корнієнко //Наукоємні технології. — 2012, № 3 (15), С. 83–89, doi.org/10.18372/2310-5461.15.5120 (ukr).

2. **Korniyenko B. Y.** Open systems interconnection model investigation from the viewpoint of information security / B. Korniyenko, O. Yudin, E. Novizkij // The Advanced Science Journal, 2013. — issue 8. — P. 53–56.

3. **Корнієнко Б. Я.** Реалізація інформаційної безпеки у моделі взаємодії відкритих систем / О. К. Юдін, Б. Я. Корнієнко: збір. тез VI Міжнародної науково-технічної конференції «Комп'ютерні системи та мережні технології» (CSNT-2013), 11–13 червня 2013 р. — С. 73.

4. **Корниенко Б. Я.** Информационная безопасность и технологии компьютерных сетей : монография / Б. Я. Корниенко // LAMBERT Academic Publishing, Saarbrucken, Deutschland, 2016. — 102 c.

5. **Korniyenko B**. Modeling of security and risk assessment in information and communication system / B. Korniyenko, L. Galata, O. Kozuberda / Sciences of Europe. — 2016. — V. 2. — No 2 (2). — P. 61–63.

6. **Korniyenko B**. The classification of information technologies and control systems / B. Korniyenko // International scientific journal. — 2016. — № 2. — P. 78–81.

7. Korniyenko B. Risk estimation of information system / B. Korniyenko, A. Yudin, L. Galata // Wschodnioeuropejskie Czasopismo Naukowe. — 2016. — № 5. — P. 35–40.

8. **Корнієнко Б. Я.** Безпека аутентифікації у web-ресурсах / Б. Я. Корнієнко, О. К. Юдін, О. С. Снігур / науково-практичний журнал «Захист інформації». — 2012. — № 1 (54). — С. 20–25, doi.org/10.18372/2410-7840.14.2056 (ukr).

9. **Корнієнко Б. Я.** Прикладні програми управління інформаційними ризиками / Б. Я. Корнієнко, Ю. О. Максімов, Н. М. Марутовська / науково-практичний журнал «Захист інформації», 2012. — № 4 (57). — С. 60–64, doi.org/10.18372/2410-7840.14.3493 (ukr).

Корнієнко Б. Я., Галата Л. П.

РОЗРОБКА І ДОСЛІДЖЕННЯ МАТЕМАТИЧНОЇ МОДЕЛІ СИСТЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В КОМП'ЮТЕРНІЙ МЕРЕЖІ

Наведено процес імітаційного моделювання як способу вивчення поведінки системи інформаційної безпеки. Прикладна програма Graphical Network Simulator використовується для моделювання такої системи і Kali Linux використовується для тестування на проникнення і аудит безпеки. Розглянуто основні підходи до моделювання комп'ютерних мереж. Досліджено функціональні можливості пакету GNS3. При побудові імітаційної моделі були використані основні компоненти захисту інформації. Пакет Kali Linux реалізує ряд *атак. Використовуючи моделювання при проектуванні обчислювальної системи, зроблено таке: оцінено пропускну здатність мережі та її компонентів, визначено вузькі місця в структурі обчислювальної системи; порівняно різні варіанти організації обчислювальної системи; здійснено перспективний прогноз розвитку обчислювальної системи; передбачено майбутні вимоги по пропускній здатності мережі.*

Ключові слова: математична модель, імітаційна модель, безпека, загрози, комп'ютерна мережа.

Корниенко Б. Я., Галата Л. П.

РАЗРАБОТКА И ИССЛЕДОВАНИЕ МАТЕМАТИЧЕСКОЙ МОДЕЛИ СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В КОМПЬЮТЕРНОЙ СЕТИ

В статье приведены процесс имитационного моделирования как способа изучения поведения системы информационной безопасности. Приложение Graphical Network Simulator используется для моделирования такой системы и Kali Linux используется для тестирования на проникновение и аудита безопасности. Рассмотрены основные подходы к моделированию компьютерных сетей. Исследованы функциональные возможности пакета GNS3. При построении имитационной модели были использованы основные компоненты защиты информации. Пакет Kali Linux реализует ряд атак. Используя моделирование при проектировании вычислительной системы, сделано следующее: оценено пропускную способность сети и ее компонентов, определены узкие места в структуре вычислительной системы; различные варианты организации вычислительной системы; осуществлен перспективный прогноз развития вычислительной системы; предусмотрено будущие требования по пропускной способности сети.

Ключевые слова: математическая модель, имитационная модель, безопасность, угрозы, компьютерная сеть.

Korniyenko B. Y., Galata L. P.

DESIGN AND RESEARCH OF MATHEMATICAL MODEL FOR INFORMATION SECURITY SYSTEM IN COMPUTER NETWORK

This article presents simulation modeling process as the way to study the behavior of the Information Security system. Graphical Network Simulator is used for modeling such system and Kali Linux is used for penetration testing and security audit. The main approaches to simulation of computer networks are considered. The functional capabilities of the GNS3 package are explored. When building an imitation model, the main components of information protection were used. The Kali Linux package implements a number of attacks. Using simulation in the design of computer systems done the following: estimated bandwidth network and its components identified bottlenecks in the structure of computer systems; compared different options for computer systems; made a promising forecast for the development of computer systems; provides future requirements for bandwidth.

Keywords: mathematical model, simulation model, security, threats, computer network.

Стаття надійшла до редакції 19.05.2017 р.
Прийнято до друку 21.05.2017 р.
Рецензент – д–р техн. наук, проф. Щербак Л. Д.