Ministry of education of the Republic of Belarus

Educational Institution

Belarusian state university of informatics and radioelectronics

UDK 004.056

Ali

Ayoob Younus

Modeling of systems for electronic data exchange in the inter-corporate networks

ABSTRACT

for the degree of master of science

on a speciality 1-98 80 01 «Methods and systems of information protection, information security»

_____

Scientific supervisor

T.V. Borbotko

Doctor of science, professor

_____

Minsk 2016

INTRODUCTION

Technologies of Electronic Data Interchange (EDI - Electronic Data Interchange), are widely used in that E-commerce, where entities mainly take part. The development of EDI started several decades ago, and it went together with the development of computer and telecommunication systems. While the growth of the use of EDI technology conditioned by the necessity of the global information systems to integrate and the efficiency of processing to increase.

Initially, the purpose of the implementation of electronic data interchange technology was the ability of structured data exchange, which had a business nature between the various commercial applications for simplifying the tasks of collection, classification, storage, retrieval, processing and transfer of information. However, the subsequent development of information technologies led the technology of electronic data exchange to a new plane of enterprise data management throughout the enterprise. This shift was due to an important feature of the electronic document that its paper analogue didn't have, namely the ability to integrate different types of information. The spheres of technology application and electronic data interchange technology office automation and document management become closer, the borders between the documents and business data exchange are erased.

The work will cover the components of EDI technologies and the basic principles of electronic data interchange systems. The security issues of EDI-systems will be discussed in details. As a result, the system of recommendations for the usage of methods and hardware-technical means to protect electronic data in telecommunications networks will be developed. Also a software tool that allows you to provide an interactive mode of learning the basic principles of the protection of EDI based on the recommendations will be developed.

Technologies of EDI are used in that spheres, where the main participants are sufficiently large enterprises and companies that use these technologies to share important documents, therefore, a violation of safety rules may result in quite big losses, including financial ones. That's why it is difficult to overestimate the importance and urgency of this issue.

GENERAL DESCRIPTION OF THE WORK

Communication of operation with large scientific programs (designs) and themes

The theme of dissertational work matches to subsection 13 «Safety of the person, a society, the state» the priority directions of scientific researches of Byelorussia for 2016-2020, confirmed by the Decision of Ministerial council of Byelorussia on March, 12th, 2015, № 190. Work was carried out in formation establishment «Belarusian state university of informatics and radioelectronics».

The purpose and research problems

The purpose of dissertational work is working out of a program complex of modeling of information safety of systems of electronic data exchange.

For object in view achievement it was necessary to carry out following problems:

1. To analyze a problem of information safety in systems of electronic data exchange;

2. To develop a program complex for modeling of information safety of systems of electronic data exchange in corporate networks.

The personal contribution of the competitor

All basic results stated in dissertational work, are gained by the competitor independently. In common published works to the author belong: definition of the purposes and statement of research problems, sampling of methods of research, direct participation in their conducting, and also machining, the analysis and interpretation of the gained results, the formulation of leading-outs.

Approbation of effects of the dissertation

Substantive provisions and effects of the dissertation were discussed at XIII Belarus-Russian scientific and technical conference "Hardware components of protection of the information" (Minsk, 2015).

Publications on a dissertation theme

By results of the examinations presented to the dissertations, 1 operation, including 1 paper in collectors of materials of conferences are published.

THE BASIC CONTENT OF WORK

In introduction the urgency of use of systems of electronic data exchange, the purpose of introduction of such technology for corporate networks of the various organizations is considered.

In chapter one . Main principles of construction of systems of electronic data exchange, feature of formation of a stream of messages between users of such system are considered. It is shown, that management of data transmission should be made both in the organization, and in an external telecommunication network.

The question of structural data presentation in an alphanumeric format concerning standard systems, such, as ANSI X12 and EDIFACT is considered X12 which are the most widespread type of systems in the USA and Canada, and systems EDIFACT of the most popular in Europe.

Electronic Data Interchange Networks are just some kinds of data networks, increasing the threat of various network attacks. These attacks, which will be described, become more numerous and malicious. This is facilitated by two main factors. Firstly, it is ubiquitous Internet penetration. Today to this network millions of devices are connected. And millions of devices will be connected to the Internet in the nearest future. That is why the likelihood of malicious access to vulnerable devices is constantly increasing. Secondly, it is a general diffusion of technology and equipment. This factor greatly increases the opportunities that are available to the attacker.

Network attacks are as diverse as the systems against which they are directed. Some attacks are very complex. Others may carry a normal operator, who doesn't even assume what are the consequences of his work. To estimate the types of attacks one should know some of the limitations, the inherent protocol TPC / IP. The Internet was created for communication between government agencies and universities to help the educational process and scientific research. The creators of this network did not know how far it will spread. As a result, in the specifications of earlier versions of Internet Protocol (IP) there were no safety requirements. So many IP implementations are initially vulnerable. But due to the fact that the original remedy for the IP has not been developed, all of its implementation have become complemented with various network procedures, services and products that reduce the risk inherent in this Protocol.

In work the review of modern attacks, characteristic for corporate networks of an information transfer, and as requirements on protection of systems of electronic data exchange is executed.

In the second chapter. To ensure the security of information in telecommunication networks various activities are held, united by the concept

"security system". Information security system - is a set of measures, software and hardware, legal, moral and ethical standards, aimed at countering threats from offenders with the aim to minimize possible damage to users and owners of the system.

Means of information security on the methods of implementation can be divided into three groups:

- software;
- hardware and software;
- hardware.

Software data protection referred to specially designed programs that implement security functions of a computer system, perform the function of restricting access for users by passwords, keys, multi-level, etc. These programs can be implemented in almost any operating system, that is convenient for users. These software tools provide a sufficiently high degree of protection of the system and have reasonable prices. By connecting this system to the network the likelihood of a security breach increases. Consequently, this method of protection is acceptable for local loop networks having no external output.

Software and hardware devices are implemented on purpose or special purpose microprocessors that do not require modifications to the circuitry when the algorithm operation is changing. These devices can also be adapted to any operating system, and have a greater degree of protection. They cost a bit more expensive (the price depends on the type of operating system). However, this type of device is the most flexible tool to make configuration changes on request. The firmware provides a high degree of protection of the local network connected to the global [9].

Hardware devices are devices in which the functional units are implemented on VLSI Systems (VLSI) with immutable algorithm functioning. This type of device is adapted to any operating system and is the most expensive in the design, imposes high technological requirements in production. These devices have the highest degree of protection, which it is impossible to penetrate and make structural or program changes. Application of the hardware is difficult because of their high cost and the static algorithm.

Software and hardware, giving hardware speed, allow at the same time easy to modify the algorithm of functioning and do not have the disadvantages of software methods.

To a separate group of measures that ensure the safety of information and identification of unauthorized queries belong the programs detected irregularities in real time.

One of the important social and ethical issues generated by increasingly expanding the use of methods of cryptographic protection of information, the contradiction between the desire of users to protect their data and messaging and a

3

desire to specialized public services to be able to access information of some other organizations and individuals to curb illegal activities.

Cryptography provides the ability to ensure the security of information on the Internet and is now actively working on the implementation of the necessary cryptographic mechanisms in the network.

In the third chapter. Members of EDI distance from each other, and the relationship between them is carried out by means of telecommunication networks. Using of special secure communications is difficult, and using public data network, especially the Internet. To ensure the protection of electronic data interchange in the transmission of messages via telecommunication networks appropriate to apply a modular protection.

At the core of the module there are two pairs of resilient firewalls that protect application servers, EDI-translators and workstations. Additional protection is provided by the provider edge routers (ISP) and the corporate network.

Member, included in the system of electronic data exchange, initiates a connection to the EDI-translator after receiving the IP-address of the server with DNS, the network is in ISP. The DNS server is on a different network to reduce the number of protocols required for the application of EDI. The first group of firewalls should pass this protocol at a specific address. The return traffic to the same channel also passes through the screen, but this EDI-translator does not need to re-initiate a connection to the Internet. Firewall blocks this route in order to limit the possibility of hackers, if they took possession of one of the EDI-compilers.

EDI-translator initiates the request to the application server, which is on the inner side of the firewall. This connection with the return traffic must also be resolved by the first firewall. As in the case of EDI-translator, server applications do not need to initiate a connection with EDI-translator or access to the Internet.

In the head questions of maintenance of safety in a network of the enterprise-participant of system EDI also are considered.

In the fourth chapter. In the work programming model of electronic data is implemented illustrating the exchange of information between system components at all stages of the transaction. The program can explore the theoretical material on the subject, and then proceed to the construction of a process data exchange with the subsequent choice of methods and means of information security at each stage. For correct operation of the program on the computer must be running shell program Macromedia Flash Player version is not below 7. The algorithm of the program contains in the dissertation text.

CONCLUSION

The work analyzes the problems of security of electronic data interchange systems, a review of the main threats to information security and means of countering them, considered the protection of EDI in telecommunication networks, based on the analysis performed to develop recommendations on the application of methods and hardware-software protection of EDI systems and developed a software implementation model of protection EDI systems, which allows to provide an interactive mode of learning the basic principles of the protection of EDI based on developed recommendations.

Because electronic data interchange is constantly evolving, and it involves a large amount of valuable information, the issue of its protection is very important. Using the proposed thesis on the use of methods and means of protection of information in electronic data exchange will ensure comprehensive protection of EDI systems to create an information security system. Developed software tools can serve in educational purposes.