Исследованы четыре этапа движения хрупко разрушаемой среды, которая по своим свойствам близка к раздробленной горной породе.

Выводы и направление дальнейших исследований. Анализируя математические модели взрывного нагружения твердой среды, необходимо отметить условность их построения [7-10]. В действительности не существует четких границ между зонами или этапами, на которых построено рассмотрение процесса. При этом до сих пор не существует общепринятой единой точки зрения на механизм взрывного разрушения. Тем не менее, рассмотренные математические модели, в силу своей физической ясности и простоты могут быть использованы для качественного анализа процессов, происходящих при взрывном разрушении горных пород.

Список литературы

1. **Власов О.Е., Смирнов С.А.** Основы расчета дробления горных пород под действием взрыва / **О.Е.Власов, С.А. Смирнов** // М.: Изд-во АН СССР, 1962. - 107 с.

2. Механический эффект подземного взрыва / **Родионов.В.Н., Адушкин В.В.** и др. / Под. ред. М.А.Садовского. - М.: Недра, 1971. - 220 с.

3. Физика взрыва / **Баум Ф.А., Орленко Л.П., Станюкович К.П**. и др./ Под. ред. К.П.Станюковича. - М.: Наука, 1975. - 407 с.

4. **Адушкин В.В., Сухотин Л.П.** О разрушении твердой среды взрывом / **В.В.Адушкин, Л.П. Сухотин** // ПМТФ,1961. - № 4. - 94-101.

5. **Седвик П., Кокс А., Гопкинс Г.** Механика глубинных подземных взрывов / **П.Седвик, А.Кокс, Г. Гопкинс** //М.: Мир, 1966. – 188 с.

6. Управление действием взрыва скважинных зарядов на карьерах / **М.Ф. Друкованный, В.С. Куц, Ильин В.Н.** // М.: Недра, 1980. – 223 с.

7. **Жуков С.А., Тищенко С.В.** Физические процессы взрывных геотехнологий / **С.А. Жуков, С.В. Тищенко** // Кривой Рог: Минерал, 2007. - 212 с.

8. **Тищенко С.В., Еременко Г.И., Малых Д.Ю**. Временные параметры взаимодействия скважинных зарядов и энергетические характеристики процесса взрывного разрушения / **С.В.Тищенко, Г.И. Еременко, Д.Ю**. **Малых**. // Гірничий вісник, 2015. Кривий Ріг. - КНУ. - Вип. 100. - С. 22-27.

9.**Тищенко С.В., Еременко Г.И., Малых Д.Ю.** Формирование полей напряжений при взрыве скважинных зарядов ВВ в разрушаемом объеме горных пород / **С.В.Тищенко, Г.И. Еременко, Д.Ю**. **Малых**. // Вісник Криворізького національного університету, 2016. - Вип. 43. - С. 153-158.

10. **Тищенко С.В., Еременко Г.И., Малых Д.Ю.** Эффективность использования энергии взрыва при взрывании скважинного заряда взрывчатыми веществами / **С.В.Тищенко, Г.И. Еременко, Д.Ю**. **Малых**. // Гірничий вісник, 2014. - Кривий Ріг. - КНУ. - Вип. 97. - С. 19-21.

Рукопись поступила в редакцию 09.04.2018

UDC 004.056.52:334.78

N. O. KARABUT,[*] Senior Lecturer, D. V. SHVETS, Teaching Assistant,
S. O. LUKASH, Undergraduate Student
Kryvyi Rih national university

SAFE CORPORATE NETWORK ACCESS

Purpose. To analyze existing techniques and means of improved security corporate network data and to identify weak links of hardware and software which can threaten the data security and network functionality. The data security in corporate networks is an urgent issue due to the rapid increase in the number of incidents of information technology. Many of them were confronted with a wide range of private, corporate and governmental interests.

Methodology. Existing methods for organizing a corporate network, as well as methods for improving security data transmission and storage are as follows: access control to network resources, network connection, (DMZ) demilitarized zone, network segmentation, service division into Front- and Back- ends. Comparative analysis of the corporate networks in view of design characteristics, their pros and cons is provided**.**

Scientific novelty. The methods of data protection in corporate networks that exist today, and further develop of new methods to improve the security of corporate systems, which reduce the vulnerability of corporate networks and increase the confidentiality of data transmitted, are analyzed.

Practical value. Main incidents and a number of possible solutions to the problem of data security in corporate networks and means of preventing attacks of cybercriminals on information systems, which increase the security of corporate networks are considered.

Results. Considered software and hardware means to ensure an appropriate security of corporate networks are of a great significance in the use today. The following analysis allows us to further synthesize new methods of protecting corporate networks.

Keywords: corporate networks, information security, data protection.

doi: 10.31721/2306-5435-2018-1-104-47-50

The issue and its connection with scientific and practical tasks. Nowadays a rapid increase in the number of incidents in a field of information security takes place, which have a wide dissemination and are of an increasing threat.

Many of those attacks interfere with a wide range of private, corporate and governmental interests.

The main trends in the growth of those threats include:

the increase of number of attacks that lead to heavy losses;

the increase in a complexity, which involves several stages and uses special methods of protection to deny counter-actions;

the impact on almost all electrical appliances, including portable devices, which are of an increasing importance and vulnerability in the field of information security;

the more frequent cases of attacks targeting the information infrastructure of large corporations, important industrial facilities and governmental structures;

All of the above demonstrates the importance of safe storage and transfer of information within corporate networks. The presence of software and hardware vulnerabilities in such networks is a significant threat and can lead to unauthorized access to information and/or its falsification and, as result, to financial and reputational losses of the company.

Modern corporate networks provide the functionality of different kind of services. Among which are: traditional data transmission, mail and terminal service, network printers, video surveillance. Usage of corporate networks within the organization provides an efficient work of users and a convenient access to them, shorten working hours and increase overall efficiency of company management.

However, it is important to consider that usage of global connectivity in corporate networks implies a high importance of information security implementation. It is connected to a dispread and constantly circulating nature of information inside corporate networks which leads to a necessity to avoid possible unauthorized access through vulnerabilities of such network.

Analysis of research and publications. In corresponding literature and web-resources various methods to organize corporate network are considered. As well as techniques targeted at the increase of a security level within corporate information transmission channels. However, in most cases, described methods are not complete and don’t provide enough universality. As a result, causing and urgent need in detailed classification of existing methods and tools, used to organize an information space of corporations and configure services of corporate networks.

Problem statement. To classify options of organizing a secure access to services of corporate network through the Internet, considering possible differences in the architecture of systems and variations in attacks’ targets and methods.

Material presentation and results. To organize a secure access to services of a corporate network through the Internet a number of ways to configure it are advised. One of them is A flat network, when all nodes of a corporate network are linked to one internal network, shared by all clients with unlimited and uncontrolled internal interconnections. However, this method doesn’t provide a required level of security. To address this issue, nodes of the network, that can be accessed from the Internet are placed in a special dedicated segment – a demilitarized zone (DMZ). Demilitarized zone is organized with a help of firewalls, which separate it from the Internet and from the rest of the internal network. Firewall filtration rules are as follows: it’s possible to initialize a connection from internal network to a DMZ and to a WAN (Wide Area Network), from DMZ to WAN, from WAN to DMZ. Initialization of connections from WAN and DMZ to the internal network is prohibited.

This variant increases the protection from hacking individual services. In case of one server being hacked, an intruder will have no access to the rest of the network. However, moving servers to DMZ on its own does not increase their security. Furthermore, the implementation of such a method require an additional firewall to separate the DMZ from the internal network.

Another way to organize a network is service separation to Front-End and Back- End. As soon as placing a server in DMZ does not improve its security, one of the possible ways to improve it is to split the functional of a server into two parts: Front- End and Back- End. Each part is placed on a separate server, servers are interconnected. Front-end servers, which implement the functional of client interaction through the Internet, are placed within the DMZ. Back- End servers, in turn, implement another type of functional and are left within the internal network. To guarantee Front-to-Back connectivity a set of rules is implemented.

At most times during an implementation phase companies choose the simplest way of service deployment and set up all its components on a single server. Then, as awareness of the need in information security grows, the functional of a services is divided into parts. The one responsible for client handling through the Internet is placed on a separate server (Front-End), which interacts with the rest of a functional (Back-End). In this setup Front-End part is placed in a DMZ, while Back-End continues to be a part of an internal segment of the network. For their intercommunication several rules are applied, which allow connection initialization between Front and Back ends.

Therefore, attacks, targeting the server, which have been organized and protected in such a way, can be eliminated at Front-End stage, which allows to minimize or to completely avoid any possible losses. For instance, DDoS-attacks, targeting the service, will lead to inaccessibility of Front-End server. At the same time letting the Back-End function correctly and service the clients. Back-end server might loss its connection to the Internet, which, in case of the service being hacked, will make it harder or almost impossible to be gained access to by intrudes. More than that, Front-End is suitable for establishing firewalls on the levels of application and intervention avoidance.

At the same time, it should be taken into account, that the rule to allow to initialize the interconnection between DMZ and the inner network must be created, which is a source of threat from a DMZ side. It should also be noted, that not all services can be divided into Front-End and Back-End components. More than that, company shall implement certain protection mechanisms to confront possible attacks from intruders, who have gained access to the DMZ.

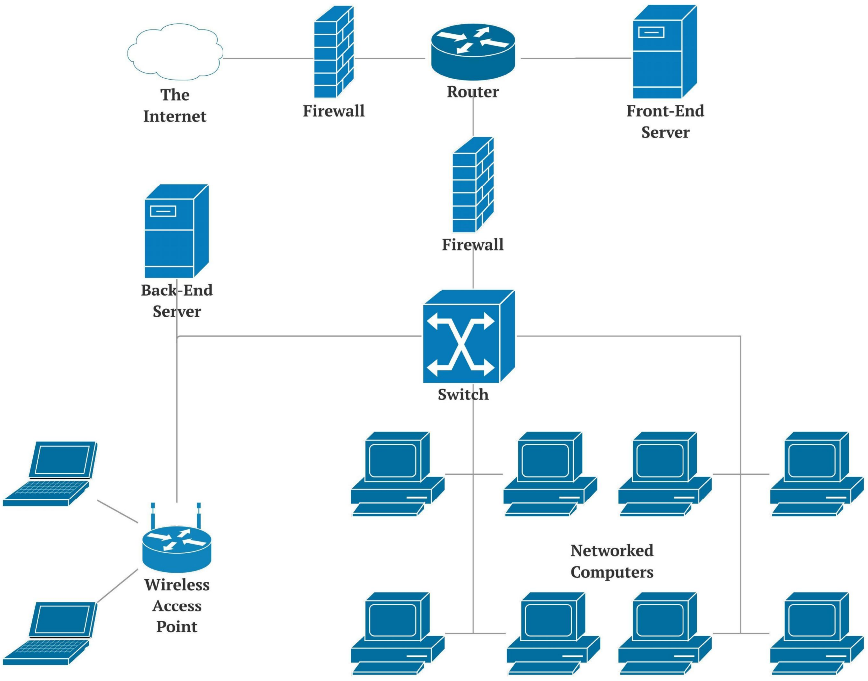

Fig. 1. Service separation to Front-End and Back- End

The extended variant of a DMZ network is a protected DMZ. Demilitarized zone, being directly accessible from the Internet, is at a higher risk of compromise of its nodes. Methods, being used in DMZ shall provide maximum redundancy in the case of intruder gaining access to one of the DMZ nodes. There are plenty of possible attacks that affect almost all systems that operate on manual settings. Some of them are: authentication bypassing, password brute forcing, exploiting vulnerabilities of network services, attacking Web-applications, etc. Part of attacks is based on Ethernet networks vulnerabilities, which allow MAC and IP spoofing. MAC spoofing can be prevented by enabling

MAC-filtering on a routing device. IP spoofing protection, in turn, can be implement by segmenting the IP pool of the DMZ into smaller sub-pools and filtering all incoming connections.

Due to the large number of possible attack variations there is no universal solution to be found. Every particular case requires individual security configurations to be implemented. Traditional methods of addressing vulnerabilities are: implementing vulnerability management procedures, installing patches and using an intrusion prevention system.

Usage of a protected DMZ significantly increases the security level of a corporate network, but on the other hand requires more functional hardware and more time-consuming installation and maintenance process.

Conclusion. Options of organizing access to the corporate network, mentioned above, increase the security of transmission and storage of corporate information. A choice of each individual method is determined by the value of information, being protected, technical resources, which the company possesses and the qualification of specialists, which are responsible for system implementation and maintenance.

References

1. **Eric Maiwald**. Network Security, - McGraw-Hill Education; 3 edition. - 2012. - p.336

2. **Kurose, James F.** Computer networking: a top-down approach / **James F. Kurose, Keith W. Ross.** - 6th ed., - 2016. - p. 862

3. **Бирюков А.А.** Информационная безопасность: защита и нападение, - ДМК Пресс, 2016. – 536 с.

4. **Mark Ciampa.** CompTIA Security+ Guide to Network Security Fundamentals - Cengage Learning, 6 edition. – 2017. - p.720

5. **Michael T. Simpson**. Hands-On Ethical Hacking and Network Defense. - Cengage Learning, 3 edition. – 2016. – p.512

6. **Michael Sikorski.** Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software – 2012 – p.800

7. **Erdal Ozkaya.** Cybersecurity – Attack and Defense Strategies: Infrastructure security with Red Team and Blue Team tactics / E. Ozkaya, Y. Diogenes - Packt Publishing. – 2018. – p. 384

8. **Олифер, В. Г.** Безопасность компьютерных сетей / **В. Г. Олифер, Н. А. Олифер.** - М: Горячая линия-Телеком, 2016. – 643 с.

9. **Польман Н., Кразерс, Т.** Архитектура брэндмауэров сетей предприятия: Пер. с англ. – М.: Издательский дом «Вильямс», 2003. – 432 с.

10. **Грайворонський М. В., Новіков О. М.** Безпека інформаційно-комунікаційних систем. – К.: Видавнича група BHV, 2009. – 608 с.

11. **Крэйг Хант.** TCP/IP. Сетевое администрирование, 3-еиздание. - Пер. с англ. - СПб: Сим-вол-Плюс, 2007. - 816 с.

12. **Тимошенко А. О.** Методи аналізу та проектування систем захисту інформації: Курс лекцій. – К.: Політехніка, 2007. – 174 с.

13. **Шеховцов В. А.** Операційні системи – К.: Видавнича група BHV, 2005. – 576 с.

14. **Паркер Т., Сиян К.** TCP/IP. Для профессионалов. 3-е изд. СПб.: Питер, 2004. - 859 с.

15. **Фейт С.** TCP/IP: Архитектура, протоколы, реализация: пер. с англ. – 2-е изд. – М.: Лори, 2000 . – 424 с.

The editorial board received a manuscript on 19.04.2018

УДК 332.32

В.Д. СИДОРЕНКО,[*] д-р техн. наук, проф., А.Ю. ПАЛАМАР, канд. техн. наук, доц.,
В.В. ХАРЕВСЬКА, магістрант
Криворізький національний університет

ТЕОРЕТИКО-МЕТОДИЧНІ ЗАСАДИ ЩОДО ВСТАНОВЛЕННЯ МЕЖ ЗЕМЕЛЬНИХ ДІЛЯНОК НА ЯКІ РОЗПОВСЮДЖУЄТЬСЯ ПРАВО ЗЕМЕЛЬНОГО СЕРВІТУТУ

Мета. Мета статті полягає в обґрунтуванні та аналізі теоретичних і практичних рекомендацій при обстеженні, вишукуванні, топографо-геодезичних, картографічних, проектних та проектно-вишукувальних роботах, що виконуються з метою складання документації із землеустрою. У зв'язку із залученням у цивільний оборот земельних ділянок досить складним правовим явищем виступає система земельних сервітутів.

Сервітут є одним з видів прав на чужі речі, який може бути визначений як право обмеженого користування ними (майном), встановлене в інтересах певної особи. Сервітут належить до прав, що підпорядковують річ уповноваженій за ним особі (сервітуарію) у певному напрямі і з певною метою. Сервітут дозволяє сервітуарію користуватися природними