вдається отримати необхідні функціональні залежності в аналітичній формі.

Можна зробити висновок, що для дослідження радіосистеми також потрібно використовувати багато математичних моделей, які слід проводити на базі сучасних комп'ютерних систем, а потім розробляти конкретні користувальницькі інтерфейси для кожного функціонального блоку та всієї системи [1].

Список використаних джерел:

1. Застосування технології LTE у системах реального часу – 2009. – URL: http://jrnl.nau.edu.ua/index.php/SBT/article/-view/5242/5784 (дата звернення: 18.11.2020)

Ключові слова: технологія LTE, технологія 3G, радіочастнотний спектр, радіоінтерфейс, антенні системи MIMO, WIMAX, W-CDMA, OFDM, Evolved UMTS Terrestrial Radio Access (E-UTRA), SC-FDMA.

Ключевые слова: технология LTE, технология 3G, радиочастотный спектр, радиоинтерфейс, системы антенн MIMO, WIMAX, W-CDMA, OFDM, наземный радиодоступ Evolved UMTS (E-UTRA), SC-FDMA.

Keywords: LTE technology, 3G technology, radio frequency spectrum, radio interface, MIMO, WIMAX, W-CDMA, OFDM, Evolved UMTS Terrestrial Radio Access (E-UTRA), SC-FDMA.

***Науковий керівник**: д. фіз.-мат. н., професор Василенко М. Д.*

Yurganov Vladislav Yurievich.
National University «Odessa Law Academy»,
4th year student of the Faculty of Cybersecurity
and Information Technologies

DATA PROTECTION IN COMPUTER NETWORKS

It is no coincidence that data protection in computer networks is becoming one of the most pressing problems in modern computer science. To date, three basic principles of information security have been formulated, which should ensure [1].

- data integrity;
- confidentiality;
- availability.

When considering the problems of data protection in the network, first of all, the question arises about the classification of failures and violations of access rights that can lead to the destruction or unwanted modification of data. Among these potential «threats» are:

1. Loss of information due to incorrect software operation:
– failures of servers, workstations, network cards;
– loss or change of data in case of software errors.
2. Unauthorized access losses:
– losses when the system is infected with;
– unauthorized copying, destruction or forgery of information.
3. Hardware failures:
– cable system failures;
– power outages;
– failures of disk systems;
– failures of data archiving systems.
4. Errors of service personnel and users:

– familiarization with confidential information constituting a secret of unauthorized persons or accidental destruction or modification of data.

Depending on the possible types of network disruptions (by disruption, we also mean unauthorized access), numerous types of information protection are combined into three main classes:

– physical protection means, including means of protection of the cable system, power supply systems, archiving means, disk arrays, etc.

– software protection tools, including: anti-virus programs, systems of differentiation of powers, software access control.

– administrative security measures, including control of access to premises, development of a firm's security strategy, contingency plans, etc.

The cable system remains the main problem of most local area networks: according to various studies, it is the cable system that is the cause of more than half of all network failures [2]. In this regard, the cabling system must be given special attention from the very moment of network design.

Improving the reliability and data protection in the network, based on the use of redundant information, is implemented not only at the level of individual network elements, such as disk arrays, but also at the network operating system level. So, over the past ten years, Novell has been implementing fault-tolerant versions of the Netware operating system – SFT (System Fault Tolerance), which provide for three main levels:

– SFT Level I. The first level provides, in particular, the creation of additional copies of FAT and Directory Entries Tables, immediate verification of each newly written data block to the file server, as well as backup on each hard disk about 2% of the disk space. If a failure is detected, the data is redirected to the reserved area of the disk, and the bad block is marked as bad and is not used in the future.

– SFT Level II additionally contained the ability to create «mirrored» drives, as well as duplication of disk controllers, power supplies and interface cables.

– The SFT Level III version allows the use of duplicated servers in the local network, one of which is the master, and the second, containing a copy of all information, comes into operation in the event of a master server failure.

The main and most common method of protecting information and equipment from various natural disasters (fires, earthquakes, floods, etc.) consists in storing archival copies of information or in placing some network devices, for example, database servers, in special protected premises located as a rule, in other buildings or, less often, even in another area of the city or another city.

The problem of protecting information from unauthorized access has become especially acute with the widespread use of local and, especially, global computer networks. It should also be noted that often the damage is caused not because of malicious intent, but because of elementary user errors that accidentally spoil or delete vital data. In this regard, in addition to access control, a necessary element of information protection in computer networks is the differentiation of user rights.

By equipping the server or network workstations, for example, with a smart card reader and special software, you can significantly increase the level of protection against unauthorized access. In this case, to access the computer, the user must insert a smart card into the reader and enter his personal code. The software allows you to set multiple levels of security, which are managed by the system administrator. A combined approach with the introduction of an additional password is also possible, with special measures taken against interception of the password from the keyboard. This approach is much more reliable than using passwords, because if the password is snooped, the user may not know about it, but if the card is missing, you can take action immediately.

Access control smart cards allow you to implement, in particular, functions such as access control, access to personal computer devices, access to programs, files and commands. In addition, it is also possible to carry out control functions, in particular, registration of attempts to violate access to resources, use of prohibited utilities, programs, DOS commands.

It is clearly not enough technical solutions (hardware or software) to organize reliable and safe operation of complex local networks. A single comprehensive plan is required, which includes both a list of daily security measures and urgent data recovery in case of system failures, as well as special action plans in emergency situations (fire, power outages, natural disasters). Most financial institutions in Western countries have specially developed and constantly updated security plans.

List of sources used:

1. Warwick Ford Computer Communications Security. Principles, Standard Protocols and Techniques. PTR Prentice Hall, 1994, 500 p.

2. Regis J. Bates Physical protection. In Disaster Recovery for LANs, 1994, McGraw-Hill, Inc, pp. 44-65

Key words: software, hardware, unauthorized, administrator.

Ключевые слова: программное обеспечение, оборудование, несанкционированный, администратор.

Ключові слова: програмне забезпечення, обладнання, несанкціонований, адміністратор.

***Науковий керівник**: к.т.н., доцент Бойко В. Д.*