TELECOMMUNICATION SYSTEMS AND NETWORKS

DOI 10.20535/2411-1031.2021.9.1.249831
UDC 004.056.53

OLEH KOPIIKA,
OLEKSANDR SHAPOVAL

ARCHITECTURE FOR ENSURING THE SECURITY OF MODERN IT INFRASTRUCTURE OF THE ENTERPRISE

The methodical bases of designing the security architecture of the IT infrastructure of the enterprise are considered. The architecture of the security system provides the necessary level of IT assets protection by describing approaches to the organization and formation of requirements for personnel, processes and technologies. The task of IT security is to ensure the protection of valuable information and its availability to authorized users. The security architecture includes three components: the process of risk management discipline; network zoning; echelon protection. The first component is based on the discipline of risk management. The process consists of four successive steps: identification and valuation of IT assets; identification of security risks; security risk analysis; reducing security risks. The second component is echelon protection – we assume that countermeasures are created at five levels of IT infrastructure: physical access; networks; nodes; at the data level; at the application level. The third component is network zoning. IT infrastructure is logically divided into zones with different components and protection requirements – the private zone contains assets that are fully controlled; the public area contains assets with which external customers interact. The architecture of the IT infrastructure security defines the fundamental principles of building IT services and their relationship. Security services consist of: perimeter security services, certificate management services. The perimeter security service monitors the flow of network traffic between two network segments, and provides: protection of internal servers from network attacks; implementation of network zoning, access policies and network use; traffic monitoring and detection of malfunctions. The Certificate Management Service is responsible for managing the lifecycle of security certificates used in cryptographic information security and digital signature systems. The certificate service, in particular, ensures the use of: digital signature; smart cards for user authentication; secure mail; software authorization; use of IPSec protocol; use of an encrypted file system; use of SSL and TLS protocols at the enterprise. When developing an IT infrastructure security architecture, we highlight the following criteria for quality assessment: the relationship between architectures, manageability, performance, consolidation, interoperability, and standardization.

Keywords: data center, security systems architecture, availability, digital data protection and management.

Problem statement. Technology is at the heart of almost every aspect of a modern enterprise, from organizing employees workflow to operating activity, product manufacturing and provision of services [1].

Flexible, reliable and secure IT infrastructure helps the enterprise achieve its goals and gain a competitive advantage in the market. However, mistakes in the implementation of IT infrastructure can lead to interoperability, productiveness and security, including system crashes and data leakage. Properly implemented infrastructure can be seen as a determinant of business profitability [2].

IT infrastructure is a complex of interconnected information systems and services that ensure the functioning and development of enterprise information communication tools [3].

Analysis of recent researches and publications. According to the ITIL Foundation Course Glossary, IT Infrastructure can also be termed as “All of the hardware, software, networks,

facilities, that are required to develop, test, deliver, monitor, control or support IT services. The term IT infrastructure includes all of the Information Technology but not the associated People, Processes and documentation" [4]. Leaders and managers within the IT field are responsible for ensuring that both the physical hardware and software networks and resources are working optimally. IT infrastructure can be looked at as the foundation of an organization's technology systems, thereby playing an integral part in driving its success [5]. With the current speed that technology changes and the competitive nature of businesses, IT leaders have to ensure that their IT Infrastructure is designed such that changes can be made quickly and without impacting the business continuity [6]. While traditionally companies used to typically rely on physical data centers or colocation facilities to support their IT Infrastructure, cloud hosting has become more popular as it is easier to manage and scale. IT Infrastructure can be managed by the company themselves or it can be outsourced to another company who has consulting expertise to develop robust infrastructures for an organization [7].

Regardless of the choice of the IT infrastructure option for an enterprise, it is relevant to develop a strategy for the development of the Corporation's IT infrastructure based on the use of advanced methodologies and concepts from leading manufacturers of hardware and software [8].

The following principle of building an IT infrastructure is proposed: IT infrastructure architectures define a set of services. IT services are provided to three groups of clients. IT services and clients are connected by 5 implementation scenarios. The integration of IT services is determined by 5 architectures [9]. As IT Services, we understand information technology aimed at maintaining the following elements in good technical condition: network devices, computing technique, storage devices, automatic software deployment services, network services, perimeter security services, directory services, file and print services, data management services, business application services, IT management services, archiving and recovery services, certificate management services, integration services [10], [11]. All clients of the Corporation are divided into three main groups. If necessary, clients are divided within each category separately: employees, partners and partner organizations, external consumers.

Implementation scenarios: data center (DC), department, remote office, extranet, Internet data center.

Architectures: security, management, data storage, software applications, network.

One of the most important Architectures is Security System Architecture.

The main material research. The purpose of the article is to develop a methodological framework for designing a security architecture for an enterprise IT infrastructure.

The task of IT security is to ensure the protection of valuable information and ensure its availability to authorized users. Failure to perform the security task may result to:

1. Delete or change information.
2. Theft of information or service
3. Violation of business operations.
4. Damage to the company's reputation.

The security architecture provides the necessary level of protection of the company's IT assets by describing approaches to the organization and formation of requirements for personnel, processes and technologies.

The corporate infrastructure must be in compliance with ISO/IEC 27001 "Information technology. Security techniques. Information security management systems. Requirements". Data center policies developed in accordance with these standards can provide the necessary level of staffing, processes and technologies to ensure the proper use of IT assets by authorized users [12].

The security architecture is developed on the basis of three components:

1. The process of risk management discipline.
2. Network zoning.
3. Echelon protection.

IT assets

IT assets – resources have value for the work of the Corporation. IT assets include, two components – data (information, information service) and levels.

The security architecture provides data (or information) protection:

1. Confidential. Protection against unauthorized access and usage of information.
2. Integrity. Protection against unauthorized, unintentional modification or damage of information.
3. Availability. The data center must provide information and all services in a timely manner, for certain clients.

Levels are a set of nodes or devices that have the same type of functionality and can be considered as one logical component.

Staff

Basic safety principles for staff:

1. Created and used security policy. Створюються і використовуються політики безпеки.
2. The staff is enough qualified to protect the IT assets they work with.
3. Staff know about security policies and changes.
4. There are mechanisms to authenticate users and authorize their actions with data.
5. Administrators and commissions have the ability to audit actions and monitor policy implementation.

The process of risk management discipline

The security architecture includes one process that is based on the Security Risk Management Discipline (SRMD). The process consists of four consecutive steps.

1. Identification and evaluation of IT assets.

The definition of assets includes the classification of data used in the Subsystems.

Levels (logical groups of similar devices and nodes) are distinguished in addition to information.

Valuation of assets includes analysis of:

1. The physical cost of the IT infrastructure component:
   a) the cost of hardware;
   b) the cost of the software;
   c) maintenance and operation costs;
   d) replacement cost.
2. Business value – the value of the asset to fulfill the mission of the Subsystem.
3. Indirect cost.
4. Competitive value – the value of an asset in terms of transfer to another organization.

IT assets must be prioritized after identifiing and evaluating. Each asset is assigned an AP (asset priority) value according to which assets are sorted. Factors influencing the formation of an ordered linear list:

1. The value of the asset.
2. The price of its creation.
3. The price of its protection.
4. The price of its support.
5. The price of its restoration.
6. Asset value for competitors.

The result of the first step of the process will be four documents:

1. List of classified data.
2. List of classified levels.
3. List of valued assets.
4. List of assets that have priority.

2. Identification of security risks.

The identification of security risks is based on the following terms:

1. Threat – a potential danger, person, thing or event that threatens the safety of the asset.

2. The threat – the kind of threats – criminal, hacker, fire, earthquake.
3. Vulnerability – hardware, software, procedural point is convenient for an attack by a threat agent.
4. Attack method (exploit).
5. Risk – the value of the function that links the asset, threat, vulnerability and method of attack.

Risk identification includes:

1. Threat analysis. Who threatens each of the assets?
2. Assessing vulnerabilities. What are the asset vulnerabilities? What attacks have taken place in world practice? What are the consequences of these attacks?
3. Creating a list of risks (Fig. 1):

a) risk identification in the format "IF the threat agent uses a method or tool to affect the vulnerability, THEN the loss (confidentiality, integrity, availability) of the asset may result";

Figure 1 – Risk management methodology

b) etermining the level of additional risk: the level of data, applications, node, network, physical access;

c) determination of critical factors (CF) – the level of destruction of the asset in the event of a successful attack;

d) determining the level of the cost of the attack (E) – the amount of knowledge, experience, work required to perform the attack;

e) determining the level of susceptibility to this type of attack (VF) is a factor that allows you to associate different assets with one type of attack.

4. Risk assessment – the process of quantitative risk assessment.

The result of the second step of the process will be three documents:

1. List of threats and methods of their implementation.
2. List of vulnerabilities.
3. Table of risks.

3. Risk analysis.

For each of the selected risk determined following parameters on the third stage:

1. Probability of risk.
2. The result of the risk (consequences).

The “Basic list of priority risks” is created as a result of the analysis of all received quantitative characteristics of risks

4. Development and risk reduction.

Only risks from the document “Main list of priority risks” are taken into account. A strategy of countermeasures is formed for each of the described risks. The result of the step will be one document: “Countermeasures Strategy”.

Network zoning

One of the good practices that helps to analyze and reduce risks are zoning network. IT infrastructure is logically divided into zones with different components and protection requirements – the private zone contains assets that are fully controlled; the public area contains assets with which external clients interact (Fig. 2).

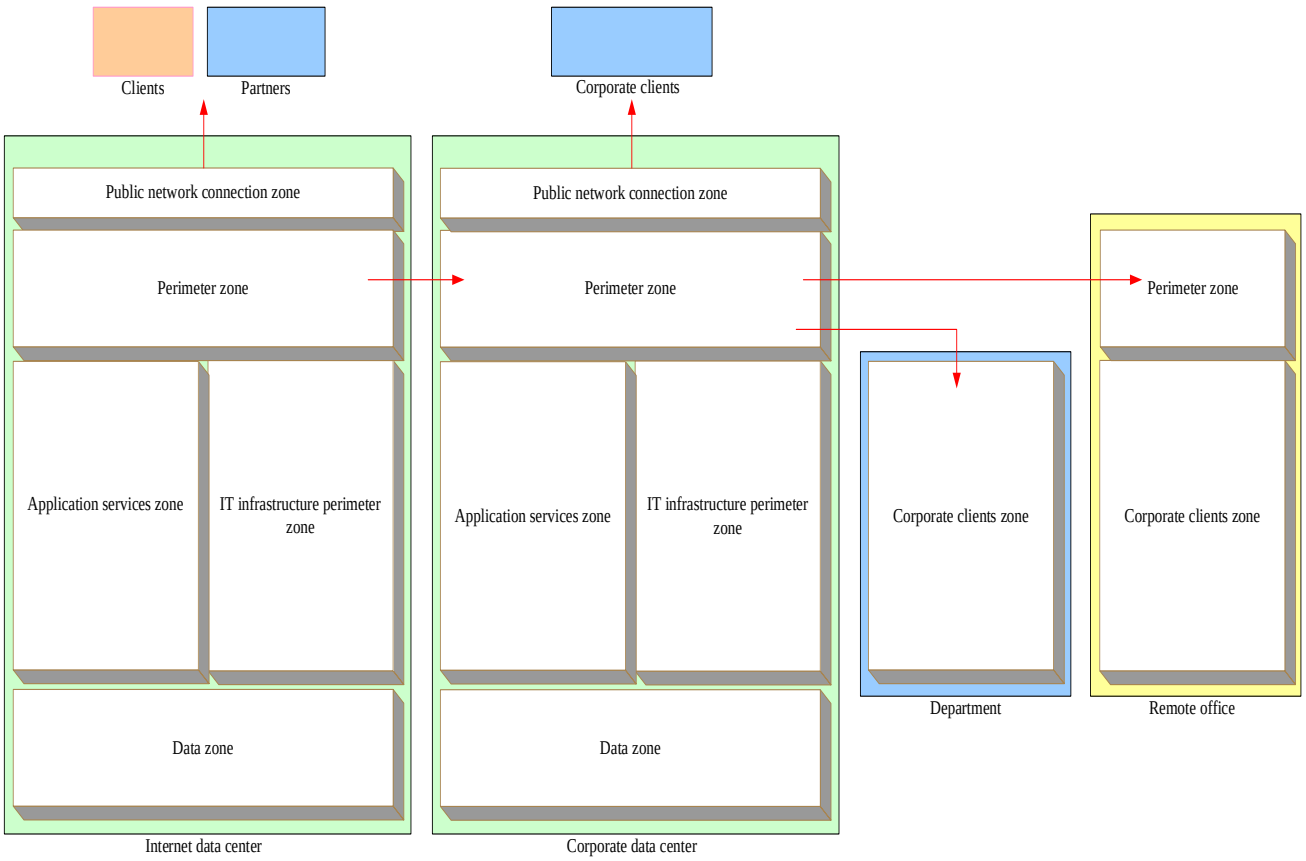

Figure 2 – Corporation network zoning

Security architecture involves using 6 security zones (Table 1)

Table 1 – Operator safety zones

Name Zones	Description
Public network connection area	Contains public network connection systems, network flow protection and inspection systems.
Perimeter area	Contains systems for remote connection, content caching, presentation-level application server.
Application area	Contains application servers and database management servers.
IT infrastructure services area	Contains security management systems, network, users and IT infrastructure.
Data Zone	Contains storage, backup and recovery systems.
Corporate customer area	Contains workstations and devices of the company's employees.

Between the zones identified and implemented the restrictions listed in Table 2.

Table 2 – Restrictions between the Operator's safety zones

Source area	Destination area	Restriction
Public	Private	A device for analyzing network packets located between the zones.
Public	Private	Only network traffic of ports 80 and 443 is allowed to pass between zones.
Public	N/A	If users authenticate themselves at any level in this zone, the layer must provide an encrypted channel for information exchange.

The second practice of risk reduction – Echelon protection - assumes that countermeasures are created at five levels of IT infrastructure (Fig. 3):

1. Level of physical access.
2. Network level.
3. Node level.
4. Data level.
5. The level of applications.

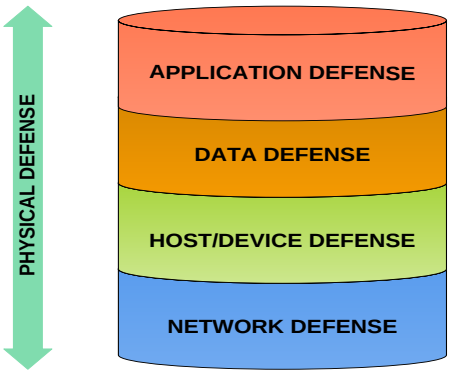

Figure 3 – Levels of echelon protection in the Corporation

Since in most cases an agent needs to use or bypass multiple layers to launch an attack, placing countermeasures at all layers can significantly reduce the risk. As an example, the Corporation's IT infrastructure must remain secure when the firewalls are disabled.

Protection technologies

Each component of the IT infrastructure includes protection mechanisms. It is advisable to highlight the list of all mechanisms in a separate Table 3.

Table 3 – Defense mechanisms

Defense mechanisms	Types of risks
Application layer	
HTML content filters	Identifies and responds to unauthorized URL strings.
Data layer	
Authorization (NTFS ACL)	Denies access to data for unauthorized clients.
Encryption (IPSec, EFS, SSL)	Reduces the risk of listening t information in the Internet and read data from data storage to bypass authentication mechanisms.
Node level	
Internet Information Services (IIS) 6.0 Hardening	Provides an additional layer of protection for the IIS 6.0 application server and helps avoid configuration errors.
Security templates	Brings the system to a basic level of security by configuring over 1200 parameters.
Network layer	
Firewalls	Firewalls provide network traffic inspection and are located between network zones.
Internet Protocol Security (IPSec)	Protects the integrity and confidentiality of network traffic.
Physical access layer	
Physical access control	Controlled access to the rooms and floors of the Corporation.
Tourniquet	Access control to the territory of the Corporation.

Management

The security architecture must be manageable and include appropriate people, processes and technology (Table 4).

Table 4 – Roles in security architecture

Role cluster	Role name
Operations, Release, Infrastructure, Support, Security	Security manager Human Resources Security Manager Operating Systems Security Engineer Hardware Security Engineer Network security engineer Physical Access Security Engineer External Contractor Manager Security auditor

When developing an IT infrastructure security architecture, we highlight the following criteria for assessing the quality of the system:

1. The relationship between architectures.

The security architecture is interconnected with all IT infrastructure architectures: management; data storage; applications; network.

2. Controllability.

Controllability is a defining feature of a security system. An unmanaged security system is very difficult to protect. Without the use of monitoring mechanisms – potential breaches of protection may go unnoticed. Without diagnosis more difficult to resolve security issues.

The approach of using zones adopted for the security system can also be used for its management. Each security zone can be considered as a management area, and security management tasks can be assigned to local administrators, if necessary.

Use of administrative roles

Roles in the Security cluster perform the following general responsibilities:

– assistance in monitoring the correctness of IT resources;

– intrusion detection and virus protection;
– providing protection by refusing service;
– determination of hiding policies and secure data transfer;
– performing an audit and reporting on its results;
– designing an effective security system and management system for network domains;
– testing and implementation of strategic protection technologies;
– monitoring and assessment of network vulnerabilities;
– providing a rapid response to intrusions in real time;
– public key infrastructure management;
– management of IP security requirements;
– management of authentication and access requirements;
– management of the application and requirements of user policies (for example, password policy);
– management of external and physical security requirements (for example, access to computer laboratories);
– management of requirements for secure messaging;
– providing ongoing technical support and advice on relevant issues for various security initiatives in the organization.

System administration

For a security manager a centralized approach to security administration is quite simple, as all tasks are concentrated in one place. However, the security architecture may make remote management impossible due to certain security limitations.

Security also depends to some extent on the remote distribution of software, including how quickly it updates the client software VPNs and antivirus programs. Systematic administration of the tools used to implement security and level protection can be a challenge. When the organization adopts a strategy of deep protection, it leads to an increase in the complexity of environmental management depending on the importance of the components.

3. Productivity.

The performance of a security system primarily depends on what technologies and constraints are implemented in the environment.

– packet filtering at the network level. In almost all situations, packet filtering increases the time it takes to transmit from source to destination. The delay depends on how the packets are checked. For example, frequent application-level proxy checks take longer than simple port filtering, as this process requires more in-depth packet research.
– encryption. Data encryption always leads to the transfer of more data, and also creates an additional load on the processors of devices that perform encryption and decryption. Such loads can be transferred to special hardware.

4. Consolidation.

What the security system will be – separate or consolidated, is determined by the network architectures and software that it supports. Facilitating the management of the security system is a determining factor in the consolidation of server and network devices. But consolidation should take into account the requirements for data security zones and structures designed to support security.

5. Interoperability.

All measures to reduce risks should be implemented as part of the security policy. There are a number of interoperability standards for technology implemented as part of a security system.

6. Standards.

ISO/IEC 27001 “Information technology. Security techniques. Information security management systems. Requirements” and other [12] - [17].

Conclusions. The IT infrastructure security architecture defines the fundamental principles of building IT services and their relationship. Also, the requirements for the creation of IT services are formed on the basis of architecture.

Security services consist of: perimeter security services (provider edge (PE) perimeter and internal, proxy/cache services), certificate management services – Public Key Infrastructure (PKI).

The firewall service monitors the flow of network traffic between two network segments. The service provides:

1. Protect internal servers from network attacks.
2. Implementation of network zoning, access policies and network use.
3. Traffic monitoring and detection of malfunctions.

PKI Certificate Management is responsible for managing the lifecycle of security certificates used in cryptographic information security and digital signature systems.

The Certificate Service, in particular, provides use in the Corporation:

1. Digital signature.
2. Smart cards for user authentication.
3. Secure Mail (S / MIME).
4. Software Authorization (Authenticode).
5. Using the IPSec protocol.
6. Using the 802.1x protocol.
7. Using an encrypted file system (EFS).
8. Use of SSL and TLS protocols.

When developing an IT infrastructure security architecture, we highlight the following criteria for quality assessment: the relationship between architectures, manageability, performance, consolidation, interoperability, standards.

REFERENCE

[1] S. Dovgiy, and O. Kopiika, "Changing business models of IT management at the nature management enterprise in connection with the development of service-oriented information technologies", *Ecological safety*, no. 1 (37), pp. 5-19, 2021, doi: https://doi.org/10.32347/2411-4049.2021.1.5-19.

[2] S. Dovgiy, and O. Kopiika, "Improving the efficiency of enterprise management through the transformation of IT infrastructure", *Mathematical modeling in economics*, iss. 1-2, pp.7-16, 2017.

[3] L. Berkman, and O. Kopiyka, "Theoretical bases methodology synthesis of information and communication systems", *Telecommunication and Informative Technologies*, no. 4, pp. 12-20, 2014.

[4] ITIL® V3 Foundation Course Glossary. [Online]. Available: https: //itil.it.utah.edu/ downloads/ ITILV3_Glossary.pdf. Accessed on: Jan 21, 2021.

[5] What is IT Infrastructure? [Online]. Available: https://www.ecpi.edu/blog/what-is-it-infrastructure. Accessed on: Jan 21, 2021.

[6] Beginner's Guide to IT Infrastructure Management. [Online]. Available: https://www.smartsheet.com/it-infrastructure-management-services-guide. Accessed on: Jan 21, 2021.

[7] What is infrastructure (IT infrastructure)? Definition from WhatIs.com. SearchDataCenter. [Online]. Available: https://searchdatacenter.techtarget.com/definition/infrastructure. Accessed on: Jan 21, 2021.

[8] S. Dovgiy, *New technologies in telecommunications: the choice of technological architecture. Modern development trends*, Kiev, Ukrtelecom, 2001.

[9] Reference architectures MSA. Kyiv, Ukraine: BHN, 2005.

[10] O. Kopiyka, "Network architecture in the modern data centers", *Scientific notes Ukrainian Research Institute of Communications,* no. 2 (30), pp. 34-41, 2014.

[11] O. Kopiyka, “Network services and network devices service in the data center”, *Control, navigation and communication systems*, iss. 4 (28), pp. 98-104, 2013.
[12] International organization for standardization. (2013, Sept. 25). *ISO/IEC 27001, Information technology. Information security management systems. Requirements*. [Online]. Available: https://www.iso.org/ru/standard/54534.html. Accessed on: Jan 21, 2021.
[13] J. Jonathan, “BICSI Data Center Standard: A Resource for Today’s Data Center Operators and Designers”, *BICSI News Magazine*, p. 28, 2010.
[14] N. Susan, ”Standardization and Modularity in Data Center Physical Infrastructure”, *Schneider Electric*, p. 4, 2011.
[15] The Telecommunications Industry Association. [Online]. Available: http://www.tiaonline.org/ standards/. Accessed on: Jan 21, 2021.
[16] The Telecommunications Industry Association. (2005, Apr. 12). *ANSI/TIA-942, Telecommunications Infrastructure Standard for Data Centers*. [Online]. Available: https://tiaonline.org/products-and-services/tia942certification/ansi-tia-942-standard/. Accessed on: Jan 21, 2021.
[17] Bylaws of the building industry consulting service international. (2019, Jan. 21). *ANSI/BICSI 002, Data Center Design and Implementation Best Practices*. [Online]. Available: https://www.bicsi.org/standards/available-standards-store/single-purchase/ansi-bicsi-002-2019-data-center-design. Accessed on: Jan 21, 2021.

The article was received 02.02.2021.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] С. Довгий, та О. Копійка, “Зміна бізнес-моделі управління ІТ на підприємстві природокористування у зв’язку з розвитком сервісно-орієнтованих інформаційних технологій“, *Екологічна безпека*, № 1 (37), с. 5-19, 2021, doi: https://doi.org/10.32347/ 2411-4049.2021. 1.5-19.
[2] С. Довгий, та О. Копійка, “Підвищення ефективності управління підприємством за рахунок трансформації ІТ-інфраструктури”, *Математичне моделювання в економіці*, Вип. 1-2, с.7-16, 2017.
[3] Л. Н. Беркман, та О. В. Копійка, “Теоретичні основи методології синтезу інформаційно-комунікаційних систем”, *Телекомунікаційні та інформаційні технології*, № 4, с. 12-20, 2014.
[4] ITIL® V3 Foundation Course Glossary. [Online]. Available: https: //itil.it.utah.edu/ downloads/ ITILV3_Glossary.pdf. Accessed on: Jan 21, 2021.
[5] What is IT Infrastructure? [Online]. Available: https://www.ecpi.edu/blog/what-is-it-infrastructure. Accessed on: Jan 21, 2021.
[6] Beginner’s Guide to IT Infrastructure Management. [Online]. Available: https://www.smartsheet.com/ it-infrastructure-management-services-guide. Accessed on: Jan 21, 2021.
[7] What is infrastructure (IT infrastructure)? Definition from WhatIs.com. SearchDataCenter. [Online]. Available: https://searchdatacenter.techtarget.com/definition/infrastructure. Accessed on: Jan 21, 2021.
[8] С. А. Довгий, *Новые технологии в телекоммуникации: выбор технологической архитектуры. Современные тенденции развития*, Киев: Укртелеком, 2001.
[9] Reference architectures MSA. Kyiv, Ukraine: BHN, 2005.
[10] О. В. Копійка, “Архітектура мережі в сучасних дата-центах”, *Наукові записки Українського науково-дослідного інституту зв’язку*, № 2 (30), с. 34-41, 2014.
[11] О. В. Копейка, “Сетевые службы и службы сетевых устройств в Дата-центрах”, Системи управління, навігації та зв’язку, вип. 4 (28), С. 98-104, 2013.

[12] International organization for standardization. (2013, Sept. 25). *ISO/IEC 27001, Information technology. Information security management systems. Requirements*. [Online]. Available: https://www.iso.org/ru/standard/54534.html. Accessed on: Jan 21, 2021.
[13] J. Jonathan, "BICSI Data Center Standard: A Resource for Today's Data Center Operators and Designers", *BICSI News Magazine*, p. 28, 2010.
[14] N. Susan, "Standardization and Modularity in Data Center Physical Infrastructure", *Schneider Electric*, p. 4, 2011.
[15] The Telecommunications Industry Association. [Online]. Available: http://www.tiaonline.org/standards/. Accessed on: Jan 21, 2021.
[16] The Telecommunications Industry Association. (2005, Apr. 12). *ANSI/TIA-942, Telecommunications Infrastructure Standard for Data Centers*. [Online]. Available: https://tiaonline.org/products-and-services/tia942certification/ansi-tia-942-standard/. Accessed on: Jan 21, 2021.
[17] Bylaws of the building industry consulting service international. (2019, Jan. 21). *ANSI/BICSI 002, Data Center Design and Implementation Best Practices*. [Online]. Available: https://www.bicsi.org/standards/available-standards-store/single-purchase/ansi-bicsi-002-2019-data-center-design. Accessed on: Jan 21, 2021.

ОЛЕГ КОПІЙКА,
ОЛЕКСАНДР ШАПОВАЛ

АРХІТЕКТУРА ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ СУЧАСНОЇ ІТ ІНФРАСТРУКТУРИ ПІДПРИЄМСТВА

Розглянуто методичні основи проєктування архітектури безпеки ІТ інфраструктури підприємства. Архітектура системи безпеки забезпечує необхідний рівень захисту ІТ активів шляхом опису підходів по організації і формуванню вимог до персоналу, процесів і технологій. Завдання безпеки ІТ полягає в забезпеченні захисту цінної інформації і її доступності авторизованим користувачам. Архітектура безпеки включає в себе три компоненти: процес дисципліни управління ризиками; зонування мережі; ешелонний захист. Перша компонента базується на дисципліні управління ризиками. Вона складається з чотирьох послідовних кроків: визначення та оцінювання ІТ-активів; ідентифікація ризиків безпеки; аналізу ризиків безпеки; зменшення ризиків безпеки. Друга компонента це ешелонний захист, за яким контрзаходи створюються на п'яти рівнях ІТ інфраструктури: фізичному доступі; мережі; вузлів; на рівні даних; на рівні прикладних програм. Третя компонента це зонування мережі. ІТ інфраструктура логічно ділиться на зони з різними компонентами та вимогами до захисту – у приватній зоні активи повністю контрольовані; у публічній зоні передбачається взаємодія зовнішніх користувачів з активами. Архітектура безпеки ІТ інфраструктури визначає фундаментальні принципи побудови ІТ сервісів і взаємозв'язок між ними. Сервіси безпеки складаються з: служби захисту периметрів, служби управління сертифікатами. Служба захисту периметра контролює потік мережевого трафіку між двома сегментами мережі, та забезпечує: захист внутрішніх серверів від мережевих атак; реалізацію зонування мережі, політик доступу та використання мережі; моніторинг трафіку і виявлення порушень в роботі. Служба управління сертифікатами відповідає за управління життєвим циклом сертифікатів безпеки, що використовуються в системах криптографічного захисту інформації та цифрового підпису. Служба сертифікатів зокрема забезпечує використання на підприємстві: цифрового підпису; смарт-карт для аутентифікації користувачів; захищеної пошти; авторизації програмного забезпечення; використання протоколу IPSec; використання шифрованої файлової системи; використання протоколів SSL і TLS. При розроблені архітектури безпеки ІТ інфраструктури виділено такі критерії для оцінки якості: взаємозв'язок між архітектурами, керованість, продуктивність, консолідація, інтероперабельність та стандартизація.

Ключові слова: дата-центр, архітектура системи безпеки, доступність, захист і управління цифровими даними.

Kopiika Oleh, doctor of technical science, senior researcher, professor at the cybersecurity and application of information systems and technologies academic department, Institute of special communication and information protection National technical university of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine, ORCID 0000-0003-0189-3915, okopiyka@gmail.com.

Shapoval Oleksandr, senior lecturer at the cybersecurity and application of information systems and technologies academic department, Institute of special communication and information protection National technical university of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine, ORCID 0000-0002-4960-2235, shapoval72@gmail.com.

Копійка Олег Валентинович, доктор технічних наук, старший науковий співробітник, професор, кафедра кібербезпеки і застосування інформаційних систем і технологій, Інститут спеціального зв'язку та захисту інформації Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського", Київ, Україна.

Шаповал Олександр Миколайович, старший викладач, кафедра кібербезпеки і застосування інформаційних систем і технологій, Інститут спеціального зв'язку та захисту інформації Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського", Київ, Україна.

DOI 10.20535/2411-1031.2021.9.1.249839
UDC 004.896

ANDRII DIVITSKYI,
SERHII SALNYK,
VLADYSLAV HOL,
ANTON STORCHAK

METHOD OF IDENTIFICATION OF DATA ROUTES IN WIRELESS SELF-ORGANIZED NETWORKS

Proposes a method for identifying data routes in wireless self-organized networks on the basis of genetic algorithms. The features of building networks of this class are described. The main tasks of the functioning of control systems of wireless self-organized networks were defined. It was emphasized that for complete functioning of wireless self-organized networks control systems was maintaining of adequate quality of their service, which included the process of changing data transmission routes and predicting the time of changes in routes. It was justified that forecasting allowed you to set up the network in time to prevent overloads, errors, failure,to predict changes in data transmission routes in different situations. The forecasting process was described. It was found out that to solve the forecasting tasks, it is advisable to use a genetic algorithm, in particular, the problems of multicritical optimization. This is due to the principle of multicritial optimization, which consists in searching for the optimal solution that simultaneously satisfies more than one target function. The routing system, its tasks and features of construction are described. The model of the forecasting subsystem is described, its importance is emphasized. The concept of identification and its methods (active, passive) are defined. It was considered the work of the rapid genetic algorithm in which due to the presence of a special elite population we can significantly reduce the time of searching for acceptable solutions on separate steps of measurements, compared to the classic genetic algorithm. The stages of the work of the rapid genetic algorithm are described and the corresponding calculations with graphical display are carried out. The essence of