5. *Driu A.* Teoryia transportnikh potokov y upravlenye ymy. “Transport”, 1972 h., str. 1-424

6. *Garbaruk A. V., Strelets M. H., Travin A. K., Shur M. L.* Sovremennyie podhodyi k modelirovaniyu turbulentnosti . SPb. Izd-vo Politehn. un-ta, 2016. 234 s.

7. *Sohatskiy A. V.* Teoretichni osnovi stvorennya aerodinamichnih komponuvan perspektivnih shvidkisnih transportnih aparativ: dis. doktora tehnichnih nauk: 05.07.01. Dnipropetrovsk. 2010. 364 s.

8. Vvedenye v matematycheskoe modelyrovanye transportnykh potokov / Hasnykov A. V. y dr. / pod red. A. V. Hasnykova. M.: MFTY, 2010. 362 s.

✧ ✧ ✧ ✧ ✧ ✧ ✧

DOI: https://doi.org/10.32836/2521-6643-2021-1-61.3
UDC 004.056.5

B. B. Stelyuk, PhD, Professor of the Department of Cybersecurity and Information Technologies, University of Customs and Finance
D. O. Tkhorzhevskyi, teacher of Computer Science & Software Engineering Department, University of Customs and Finance
N. V. Khalipova, PhD, Professor of the Department of Transport Technologies and International Logistics, University of Customs and Finance

MODELS AND METHODS OF IMPROVING THE EFFICIENCY OF WIRELESS ACCESS OF TELECOMMUNICATION SYSTEMS AND NETWORKS

The peculiarities of construction of complex information and telecommunication systems of special purpose are researched in the work, the general and special requirements to the applied telecommunication technologies are substantiated on the example of the automated territorially distributed system of the uniform regional operative and dispatching centers. To take into account certain

properties of the generated authorization keys, a comprehensive model of authorization and authentication of wireless access is proposed for the security assessment of telecommunication systems and networks. The proposed territorial distribution systems of unified regional operational control centers for special purposes are based on the deployment of wireless telecommunication systems and must meet the basic requirements of users with high mobility.

Consider the capabilities of these systems in terms of fulfilling special requirements for ensuring the security of national information resources, personal data, information with limited access and the security of communication protocols, etc. An analysis is carried out in the specification of IEEE 802.16 series standards on the use of various cryptographic protection mechanisms designed to provide various security services and security in wireless telecommunication networks, representing various attacks aimed at disrupting the operation of authentication and authorization protocols.

The communication protocols used in the deployment and use of wireless telecommunication systems that provide an increased level of security, especially regarding the issues of unauthorized interception of transmitted data and unauthorized access to various telecommunication resources, and violations associated with false authentication of devices in relation to users of certain elements of telecommunication systems.

Basic models of wireless telecommunication systems are proposed, which are deployed in accordance with the IEEE 802.16 specification and can be used to build various information systems for special purposes, including geographically distributed systems of unified regional operational control centers in Ukraine.

Key words: *security; authorization; authentication; information and telecommunication systems; wireless information network.*

В статье исследованы особенности построения сложных информационно-телекоммуникационных систем специального назначения, на примере автоматизированной территориально распределенной системы единых региональных оперативно-диспетчерских центров обоснованы общие и специальные требования к применяемым телекоммуникационным технологиям. Для учитывания определенных свойств формируемых ключей авторизации оценки безопасности телекоммуникационных систем и сетей предложена комплексная модель авторизации и аутентификации беспроводного доступа.

Ключевые слова: *безопасность; авторизация; аутентификация; информационно-телекоммуникационные системы; беспроводная информационная сеть.*

У статті досліджено особливості побудови складних інформаційно-телекомунікаційних систем спеціального призначення, на прикладі автоматизованої територіально розподіленої системи єдиних регіональних оперативно-диспетчерських центрів обґрунтовано загальні та спеціальні вимоги до застосовуваних телекомунікаційних технологій. Для врахування певних властивостей формованих ключів авторизації оцінки безпеки телекомунікаційних систем та мереж запропонована комплексна модель авторизації та автентифікації безпроводового доступу.

Ключові слова: *безпека; авторизація; автентифікація; інформаційно-телекомунікаційні системи; безпроводова інформаційна мережа.*

Introduction. The current state of informatization of various spheres of human activity requires the introduction of the latest information and telecommunication systems and technologies with a high level of quality of services, providing the necessary probability and time indicators at all stages of collection, processing and transmission of information. Particularly stringent requirements for the quality of telecommunications services in critical information systems, in which the failure of any subsystem, or the failure of certain indicators beyond the established limits is a real danger to life and health, industry, environment, banking, transport systems, etc.

Given the complexity and diversity of factors affecting the lives of Ukrainian citizens, almost any risk factor, namely: environmental conditions, man-made disasters, natural disasters, epidemiological “outbreaks”, can have extremely serious consequences for many people who find themselves in zone of development of a dangerous situation [2]. The consequences of such global problems can be minimized only through the introduction of national security, control and response systems, development and implementation of the latest systems for collecting processing and transmitting critical information, in particular, creating a territorially distributed system of single regional operational control centers based on wireless telecommunications systems of special purpose. The implementation of these tasks is the basis of national projects, which is accepted for implementation by the State Agency for Investment and Management of National Projects of Ukraine [1, 2]. The introduction of a system of unified regional operational and dispatch centers for special purposes at the national level will have the following advantages [1, 2]:

– automation of receiving calls from the population and messages from organizations that serve the population;

– obtaining information to assess the status and priority of the use of response forces, as well as forecasting the development of the operational situation;

– monitoring of mobile services deployed on emergency response vehicles;

– assessment of actions on duty and development of further recommendations, control of response time and discipline of execution;

– recording of all actions of operators, recording of negotiations, estimation of reaction time of all elements of system and participants of operation;

– ensuring effective interaction of structural units of the Emergency (Ambulance) Medical Care, the Ministry of Internal Affairs, the Ministry of Emergencies and other units;

– formation of statistical reports and provision of reference information, which allows, in particular, to take measures to prevent false calls and release the next shift from routine work.

The automated territorially distributed system of the unified regional operative-dispatching centers of special purpose is built as modular, open and expandable. The automated system can be integrated with other automated systems or take on part of the overall information load [3].

Analysis of recent research and publications. During the preparation of the preliminary feasibility study of the automated system, the world experience of implementing similar systems was studied. Their best samples were considered, the possibilities of using modern technologies and equipment were assessed, taking into account the peculiarities of their use in Ukraine [5]. Among the main advantages of the implementation of such automated systems should be noted [3, 4]:

– significant reduction of processing time and response to calls from the population;

– full automatic quality control of calls;

– reducing the number of false departures;

– uniform load distribution;

– a single information base available to all users of the system, regardless of their geographical distance;

– increasing the level of protection and loyalty of the population to the work of assistance services.

The system of communication of centers with each other, with divisions, including the district level, with mobile subscribers, etc., is two different network technology:

1. Departmental IP-network (fixed and mobile) based on packet switching, which provides:

– receiving calls from subscribers from the Internet (e-mails, IP-telephony, on-line messages);

– interaction with medical institutions, with mobile ambulance crews, including GPS data transmission;

– centralized management of the departmental IP network;

– data exchange between any point of the network, including multimedia information (voice, video, graphics, telemetry data, etc.) to be transmitted during emergency call processing, at all stages of its support, including receiving help and advisory information, coordination with various institutions, etc.;

– access to common databases from any point of the network;

– control over the stages of implementation to the Center;

– similar-statistical processing of performance characteristics of all links, etc.

2. Telephone network based on channels switching, which provides:

– receiving calls from telephone network subscribers (from fixed public network operators, mobile network operators, private operators, networks of other departments, etc.);

– telephone communication between institutions, including – communication at the level of cities and districts of the region;

– at the district level it is possible to deploy district emergency call centers based on CATS equipment with telephone operators' workplaces;

– direct telephone communication of heads of services when using special direct communication panels;

– reservation of IP-channels to UDF operators by telephone lines;

– registration of calls (including voice channels) serviced by switching equipment of CATS (digital automatic telephone exchange).

– TD TDM / IP gateway functions (including media gateway functions and signal gateway functions) to promote calls to UDF operators.

Each regional center includes an operational dispatch service (ODS), equipped with jobs for operators implemented using IP technologies. In addition, the service operators are provided with the usual telephone connection, which will serve as a backup system in case of failure / failure of the IP network.

Thus, the creation of a territorially distributed system of unified regional operational and control centers for special purposes is based on the deployment of wireless telecommunications systems, which should provide the basic requirements [3–6]:

– construction of IP-oriented telecommunication network that is based on information technologies with packet switching using IP protocols;

– high and ultra-high peak data rates to support advanced services and applications, data rates should be between 100 Mbps for users with high mobility and from 1 Gbps for users with low mobility;

– dynamically collective network resources are used to support more simultaneous connections to one base station;

– scalable channel bandwidth, high peak spectral efficiency;

– smooth process of transferring a subscriber's session from one base station to another via different networks;

– versatility and high quality of mobile services, including the provision of various multimedia services.

These requirements are inherent in the latest telecommunications wireless access systems of the so-called fourth generation (generation), or 4G for short.

The following special requirements are put forward to the additional requirements to wireless telecommunication systems of special purpose, on the basis of which the territorially distributed systems of the single regional operational and dispatching centers are deployed [5–7]:

1. Ensuring the security of state information resources.
2. Ensuring the security of personal data.
3. Protection of information with limited access.
4. Ensuring the availability and integrity of public information.
5. Ensuring the security of communication protocols.

The communication protocols used in the deployment and use of wireless telecommunications systems should provide an increased level of security, especially in matters of unauthorized interception of transmitted data, unauthorized access to various telecommunications resources, violations related to incorrect authentication of devices and system users, violations or out of the set operation modes of communication devices and individual elements of the system [5–6].

Therefore, **an important and urgent task** now is the principle of deployment of wireless telecommunications systems for special purposes. **The aim of the research** is to use the latest information technologies related to the fourth generation of digital data networks with the implementation of increased security requirements for telecommunications systems and networks at all stages of collection, processing and transmission of information.

Presenting main material. Wireless telecommunication systems have gained the most development in recent years, as they allow to provide high-speed broadband access services, and, in practice, to ensure compliance with all requirements for fourth-generation communication systems [6–8]. Their main advantage is the rapid deployment of large areas without cable laying and providing end users with high-speed communication channels. This is especially true for places with underdeveloped network infrastructure, such as new suburbs, historic city centers, etc. The IEEE 802.16 series standards are a set of standards that define Wireless Metropolitan Area Network (WMAN) and have been developed to provide wireless broadband access to fixed and mobile users [5–11]. The scheme of standards of this series is given in figure 1.

The IEEE 802.16 series standards define the radio interface for broadband wireless access systems MAC (Media Access Control) and PHY (Physical layer) with fixed and mobile subscribers in the frequency range 1-66 GHz, designed for implementation in urban distributed wireless networks. Networks based on these standards occupy an intermediate position between local area networks (IEEE 802.11x) and regional WANs (Wide Area Network), where the application of the IEEE 802.20 standard is planned [9–11].

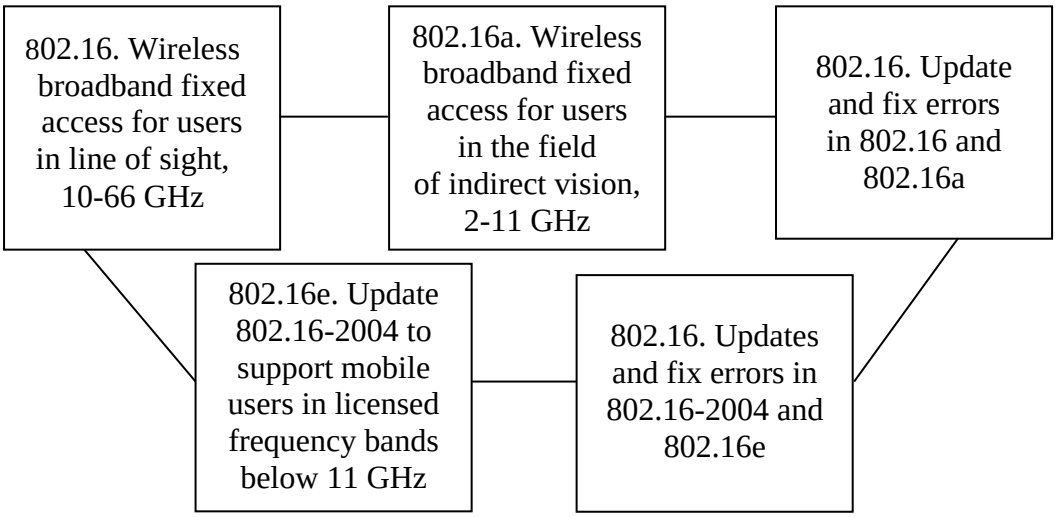

Fig. 1. Scheme of standards of the IEEE 802.16 series

These standards together with the IEEE 802.15 PAN (Personal Area Network) and IEEE 802.17 (MAC-level bridges) form a hierarchy of wireless communication standards. The standards describe the MAC and PHY levels of the reference model of open systems interaction (EMVVS - the basic reference model of open systems interaction). The level of MAC is divided into sublevel convergence, total and security. The convergence layer reconciles the top-level protocol data formats and the 802.16 MAC layer data. The data is converted into MAC SDU (Service Data Unit) packets, while the identifiers of connections, protocols and the like are formed. The general part of the MAC sublevel performs the main functions of planning, processing and allocating resources, establishing and maintaining connections, maintaining QOS (Quality of service). At the security level, data is encrypted to ensure the confidentiality of users. The physical layer determines the type of signals used for data transmission, methods of manipulation of noise-tolerant coding, algorithms for forming logical channels and so on.

Thus, the analysis shows that WiMAX (Worldwide Interoperability for Microwave Access) is a long-range system that covers large amounts of space, and which typically uses licensed frequency spectra (although possibly using unlicensed frequencies) to provide an Internet connection type point-to-point provider to the end-user. Different 802.16 family standards provide different types of access (fig. 2).

The IEEE 802.16m standard, also known as Wireless MAN-Advanced and WiMAX-2. This standard can significantly increase the bandwidth of wireless networks (stationary equipment of the new generation will receive data at speeds up to 1 Gbps, and mobile devices – up to 100 Mbps). At the same time backward compatibility with the existing WiMAX equipment remains.

A promising version of the IEEE 802.16n standard (WiMAX 3.0), which should provide the highest speed of access to networks, is planned to be adopted in the next 3–5 years. It will provide speeds for fixed channels of 10 Gbps and for mobile communications up to 1 Gbps.

The communication channel assumes the presence of two directions of transmission: ascending channel (AS–BS, uplink) and descending (BS–AS, downlink). These two channels use different frequency ranges for frequency duplex and different time intervals for time duplex.

The simplest way to represent the architecture of WiMAX networks is to describe them as a set of BS, which are located on the roofs of high-rise buildings or towers, and client transceivers. The basic model (BM) of the WiMAX network is a representation of its network architecture in the form of functional modules and standard interfaces (connection points of modules). It includes three main elements: a set of subscriber (mobile) stations (SS), a set of access networks (ASN, Access Service Network) and a set of connection networks (CSN, Connectivity Service Network). In addition, the BM includes the so-called base points (R1 ... R8), through which functional modules are connected.

An ASN belongs to a network access provider (NAP), an organization that provides access to a radio network for one or more WiMAX service providers (NSPs). In turn, the WiMAX service provider is an organization that provides IP connections and WiMAX services to end users. Within the framework of this model, WiMAX service providers enter into agreements with Internet providers, operators of other access networks, roaming agreements and the like. Service providers in relation to the subscriber can be home and guest, each with its own CSN network.

An ASN is a set of IEEE 802.16 wireless access stations and gateways for communication with a transport IP network (local or wide area networks). In fact, this network connects IEEE 802.16 radio networks and IP networks. The ASN includes at least one BS and at least one ASN gateway. But both base stations and gateways in one ASN can be several, and one BS can be logically connected to several gateways. BS in this model is a logical device that supports a set of IEEE 802.16 protocols and external communication functions.

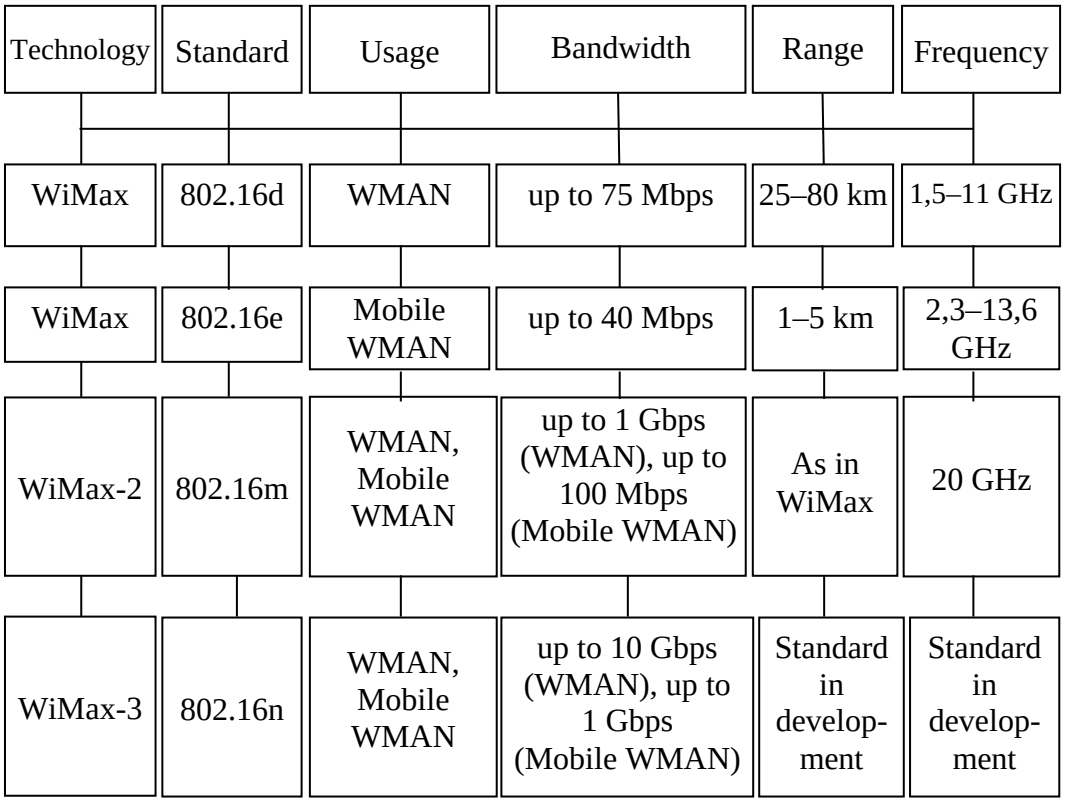

Fig. 2. Information about WiMAX standards

The analysis of the architecture and basic model of wireless telecommunication systems, which are deployed in accordance with the IEEE 802.16 specification, shows that they really meet the basic requirements for fourth generation networks and can be used to build various special purpose information systems, including geographically distributed systems. regional operational and dispatch centers in Ukraine [5–6].

Consider the capabilities of these systems in terms of compliance with special requirements for the security of public information resources, personal data, information with limited access, security of communication protocols, etc.

The most important task facing the developers of the latest wireless telecommunications systems is to ensure the protection of information at all stages of its processing and transmission through communication channels. This is due to the general availability of wireless data channels and, accordingly, the possible interception of transmitted messages. Therefore, developing the standards of wireless telecommunication systems of the IEEE 802.16 series, and especially in the IEEE 802.16e specifications, special attention was paid to the security level

[9–11]. The security layer provides authentication services (to authenticate the user and the device he uses) and authorization (to match the authenticated user to the list of services available to him). In addition, the security level of IEEE 802.16e standards meets the basic requirements of users of wireless telecommunications systems, namely confidence in the confidentiality and integrity of data transmitted over the network, as well as that the user will always be able to access paid services. Therefore, all the tasks before him are solved in three ways [8–11]:

– using the tools of the EAP protocol (Extensible Authentication Protocol) and the RSA algorithm (Rivest, Shamir and Adleman) for authentication and authorization of the SS;

– implementation of cryptographic transformations on traffic, ensuring the confidentiality, integrity and authenticity of data, as well as the authenticity and integrity of MAC-level service messages;

– using Privacy and Key Management protocol (PKM) for secure key information distribution.

A stack of protocols for the security of wireless telecoms, based on the specifics of the IEEE 802.16e standards, contains the following components [8–11]:

– PKM key management protocol in WiMAX (Worldwide Interoperability for Microwave Access) systems for the control of all components for security and key management.

– The protocols for encrypting / authenticating traffic are designed to ensure the confidentiality, integrity and authenticity of the data transmitted from the list of symmetric encryption / decryption algorithms.

– The protocols for managing operations on operating systems are designated for managing MAC-level domains linked to PKM.

– Authentication protocols are designed to perform MAC-level message authentication functions.

– RSA authentication protocols are designed to perform the authentication functions of the SS and the BS using the digital certificates X.509 contained therein, if the authorization method between the SS and the BS is selected by RSA.

–EAP encapsulation / deincapsulation protocols are designed to provide the EAP protocol interface in the event that authorization or authentication between the SS and the BS is performed using EAP.

– SA authorization / control protocols are designed to control the authorization endpoint and the data stream encryption key endpoint.

– The EAP protocol and the EAP Method protocol are outside the security level of the IEEE 802.16e standard.

It is worth noting that the PKM protocol has two versions – PKMv1 and PKMv2. Both versions are included in the IEEE 802.16e-2005, 2009 standard, but there are significant differences between them. In particular, support for the RSA algorithm is mandatory in PKMv1 and optional in PKMv2.

To transmit messages, the PKM protocol uses MAC-level service messages: PKM-REQ (uplink) and PKM-RSP (downlink). Each time one of these two messages is transmitted, the PKM message is encapsulated in it.

The analysis performed in the IEEE 802.16 series standard specification uses various cryptographic protection mechanisms designed to provide various security services. At the same time, as noted in works [3–5], the greatest threat to security in wireless telecommunications networks are various attacks aimed at violating the protocols of authentication and authorization, namely:

– the possibility of unauthorized connection of "self-proclaimed" base stations, which is due to the lack of a certificate of the base station;

– vulnerability related to non-random generation of authorization keys by the base station;

– the ability to reuse TEK (Traffic Encryption Key) keys whose life has already expired. This is due to the very small size of the EKS field of the TEK key index. Since the maximum lifetime of the authorization key is 70 days (100, 800 minutes) and the minimum lifetime of the TEK key is 30 minutes, the required number of possible TEK key identifiers is 3360. This means that the number of required bits for the EKS field is 12.

The greatest danger for security protocols are methods and algorithms for generating authorization keys, because the properties of randomness and irreversibility of these keys are based on all assumptions about the security of other security mechanisms, including traffic encryption mechanisms.

Based on the results of research and taking into account the importance and urgency of solving problems of authentication and authorization of wireless access in modern telecommunications systems and networks, we will conduct a security assessment in terms of providing reliable protection against unauthorized access to various telecommunications resources, faulty authentication and authorization of devices and users. Since authorized access in these systems is provided by generating the appropriate authorization key, the level of security will be determined based on the properties of these keys and the potential for attackers to act on them to destroy, distort, block information, its unauthorized leakage or violation of its routing. These indicators and criteria for assessing the security of telecommunications systems and networks related to the authentication and authorization of wireless access [4, 5]:

1. The probability $P_{\hat{A}}$ of exposing the rule of formation of access authorization keys. It is assessed by the criterion of minimum risk, as the highest probability of exposing the rule of forming the keys to authorize access by the attacker when applying different strategies:

$$P_{\hat{A}} = \max\{P_{\hat{A}}(v_1), P_{\hat{A}}(v_2), \ldots, P_{\hat{A}}(v_m)\}, \quad (1)$$

$P_{\hat{A}}(v_i)$ – the probability of exposing the rule of formation when applying the strategy by the attacker v_i, $V = \{v_1, v_2, \ldots, v_m\}$ – many possible strategies for

the behavior of the attacker. The lower limit is the estimate $P_{Â} \le 2^{-k}$, k – bit length of the initiation vector when generating access authorization keys.

2. The probability of coincidence $P_{Ç}$ of access authorization keys, which characterizes the number of rules for the formation of their generation, in which there is a coincidence (collision) of the generated authorization keys. The lower limit is the estimate $P_{Ç} \le 2^{-n}$, n – bit length of the generated authorization keys.

3. The probability of unauthorized access authorization $P_{íä}$, which is determined by the criterion of minimum risk by the formula $P_{íä} \le \max\{P_{Â}, P_{Ç}\}$.

4. Secure operation time $Ò_{Á}$ of access authorization keys, which is defined as the inverse of the probability $P_{íä}$ of unauthorized access authorization, taking into account the computing capabilities of the attacker:

$$Ò_{Á} = \frac{(P_{íä})^{-1}}{\gamma \cdot \Psi}, \qquad 2)$$

γ = 31 622 400 – numerical coefficient for conversion of seconds into years; Ψ – performance of the computer system, which is available to the attacker.

5. Statistical security of the scheme of formation of keys of access authorization. It is estimated by the international method of statistical testing of generators of random and pseudo-random sequences [5, 7–9] by forming a probability vector of 189 statistical tests $P = \{P_1, P_2 \ldots P_{189}\}$. The generator is considered statistically safe when all the probabilities of the vector P satisfy the set threshold, namely $\forall i : P_i \ge 0{,}96$ [5, 7–9].

We will consider the scheme of authentication and authorization of access safe if:

$$P_{Â} \le 2^{-k};\ P_{Ç} \le 2^{-n};\ P_{íä} \le \max\{P_{Â}, P_{Ç}\};\ Ò_{á} \ge \frac{(P_{íä})^{-1}}{\gamma \cdot \Psi} \qquad 3)$$

and when statistical security requirements are met.

Thus, if the inequalities in expression (3) are satisfied, the corresponding values of k and n are decisive in justifying the level of security of telecommunications systems and networks in terms of the applied authentication and authorization protocols.

Conclusions. The analysis showed that in accordance with the specification of the considered wireless telecommunication systems and networks to ensure security during authentication and authorization, modern methods and means of information protection are used to ensure high resistance to exposing the rules of

access authorization keys, i.e we will assume that the inequality $P_{\hat{A}} \le 2^{-k}$ holds. However, the experience of using wireless technologies and the large number of successfully implemented authorization violations suggests that modern requirements for the probability $P_{Ç}$ of matching access authorization keys are not met, ie the assumption $P_{Ç} \le 2^{-n}$ is incorrect. Since the remaining safety indicators are a function from $P_{Ç}$, and $P_{\hat{A}} \le 2^{-k}$, then the purpose of the work is formally written in the form of an objective function $\min(P_{Ç})$, provided that the following inequality holds $P_{\hat{A}} \le 2^{-k}$. Thus, the scientific and technical task of developing a method to increase the security of wireless telecommunications systems and networks based on the formation of pseudo-random keys for access authorization is relevant and important for the development of certain methods of data theory to improve the security of wireless telecommunications systems and networks, and in the applied sense for the construction of efficient methods and computational algorithms for the formation of pseudo-random keys for wireless access authorization.

A promising area of further research is the analysis of modern methods of forming pseudo-random sequences and substantiation of ways to build secure generators with the maximum period of formation of access authorization keys.

References:

1. Law of Ukraine "On Telecommunications" of November 18, 2003. № 1280-IV.

2. The concept of telecommunications development in Ukraine, approved by the order of the Cabinet of Ministers of Ukraine of June 7, 2006. № 316-p.

3. *Prokopovich-Tkachenko D. I.* Research of protocols of authentication and authorization of access in wireless telecommunication systems and networks // Systems of armament and military equipment, 2013, № 1 (33). P. 119–122.

4. *Prokopovich-Tkachenko D. I.* Mathematical model of authorization and authentication of wireless access in telecommunication systems and networks // Information processing systems. – Kharkiv: Kharkiv National University of the Air Force, 2013. – Edition 5 (112). – P. 111–118.

5. *Rashich A. V.* WiMAX wireless access networks: textbook. St. Petersburg: Publishing House of Polytechnic University, 2011. – P. 179.

6. Standard of wireless networks of city scale. – IEEE Std 802.16 ™. – 2009.

7. *Adibi S., Agnew G. B., Tofigh T.* End-to-End (E2E) Security Approach in WiMAX: Security Technical Overview for Corporate Multimedia Applications. P. 747–758, Handbook of Research on Wireless Security (2 Volumes) Edited By: Yan Zhang, Jun Zheng, Miao Ma, 2008.

8. *Adibi S., Lin B., Ho P.-H., Agnew G. B., Erfani S.* Authentication Authorization and Accounting (AAA) Schemes in WiMAX, University of Waterloo, Broadband Communication Research Centre (BBCR), appears in: Electro-information Technology, 2006 IEEE International Conference on 7–10. P. 210–215, May 2006.

9. Airspan, "Mobile WiMAX security", Airspan Networks Inc. 2007. [Online]. URL: http://www.airspan.com

10. *Taeshik Shon and Wook Choi*. An Analysis of Mobile WiMAX Security: Vulnerabilities and Solutions: Lecture Notes in Computer Science. Vol. 4658. P. 88–97, Aug. 2007.

11. Standard for local and metropolitan area networks. IEEE Std 802.16m-2011.

✧ ✧ ✧ ✧ ✧ ✧ ✧

DOI:
УДК 656.13(075)

О. М. Сазонець, доктор економічних наук, професор, професор кафедри транспортних технологій та міжнародної логістики Університету митної справи та фінансів
І. Ю. Леснікова, кандидат технічних наук, доцент, доцент кафедри транспортних технологій та міжнародної логістики Університету митної справи та фінансів

ДОСЛІДЖЕННЯ ХАРАКТЕРУ ПЕРЕВЕЗЕНЬ В УКРАЇНІ НА АВТОМОБІЛЬНОМУ ТРАНСПОРТІ

У статті наголошено, що автотранспорт в Україні є обслуговуючою ланкою всього національного господарства, він відіграє важливу роль у розвитку економіки країни. Представлено динаміку автоперевезень пасажирів в Україні і на її основі побудовано прогноз стану цієї галузі на наступні шість років, який є невтішним для нашої держави. Наведено причини цієї поведінки прогнозної кривої, подано способи покращання цієї ситуації, надано динаміку перевезень вантажів автомобільним транспортом в Україні, а також побудовано прогноз на майбутні шість років, який є кращим за попередній. Досліджено зв'язок між ВВП України та автоперевезеннями. Найкращою є апроксимація цього зв'язку поліномом п'ятого степеня. У дослідженні визначено основні шляхи усунення головних проблем автотранспортної галузі.