UDC: 351.862.2:004.7
DOI: 10.31110/2789-6536/2023-4/003

PROSPECTS FOR USING ASYMMETRIC CRYPTOSISM TO IMPROVE THE INFORMATION MECHANISM OF STATE MANAGEMENT OF MONITORING THE STATE OF POTENTIALLY DANGEROUS OBJECTS

Shvedun Victoriia
Doctor of Science (Public Administration), Full Professor,
Head of the Scientific Department on Problems of Management in the Civil Defence Sphere of the Educational, Scientific and Production center,
National University of Civil Defence of Ukraine, Kharkiv, Ukraine
ORCID: 0000-0002-5170-4222

Ihnatiev Oleksandr
Doctor of Philosophy (Public Management and Administration),
Senior Lecturer of the Department of Military Training,
National University of Civil Defence of Ukraine, Kharkiv, Ukraine
ORCID: 0000-0003-3280-3468

Abstract. The problems of the functioning of the information mechanism of state management by monitoring the state of potentially hazardous objects (PHO) are studied. The vulnerability of computer networks and technical means of communication (from the point of view of the reliability of transmitted messages) during the transmission of information about the state of the software was indicated. From here, the introduction of disinformation, the distortion of transmitted messages, the penetration of virus programs, including for the purpose of carrying out acts of technical terrorism, are possible.

The possibilities of using asymmetric cryptosystems in order to solve the actual problem of protecting information in the course of monitoring PHO are considered. The analysis of existing methods for protecting the integrity and reliability of transmitted messages was carried out. The prospects for the use of asymmetric cryptosystems for the transmission of messages in the collection, exchange and storage of information about the state of the software are shown. A research prototype of a program for generating an electronic digital signature is presented

The timeliness and prospects of improving the information mechanism of public administration by monitoring the state of PHO through the use of asymmetric cryptosystems have been confirmed. The advantages of using an electronic digital signature in order to confirm the reliability of information circulating in the Government Information and Analytical System for Emergency Situations are outlined.

Keywords: public administration information mechanism, monitoring, potentially dangerous object, emergency situation, asymmetric cryptographic systems, electronic digital signature.

Introduction. World practice shows that the most effective way to reduce the socio-economic consequences of emergency situations (emergency situations) of a natural and man-made nature is their prevention, which is based on constant monitoring of the state of potentially dangerous objects, which allows for information support of management decision-making procedures for the prevention of emergency situations. [1].

The effectiveness and quality of programs and plans, decision-making on the prevention and elimination of emergency situations depend on the effectiveness and quality of monitoring and forecasting. It should be emphasized that the quality of monitoring and forecasting of emergency situations significantly affects the effectiveness of activities in the field of reducing the risks of emergency situations and reducing their scale.

In order to obtain data on the current state of potentially dangerous objects and update the information contained in the database of the State Register of Potentially Hazardous Objects, these objects are monitored as part of the tasks of the unified state system for preventing and responding to emergencies of a man-made and natural nature [2]. At the same time, computer communication systems and existing technical means of communication are used to transmit information. It should be noted that, unlike closed communication channels, existing computer systems are very vulnerable in terms of the reliability of transmitted messages. Due to the openness of data transmission channels, as well as the availability in equipping with modern models of terminal communication equipment, it becomes possible to introduce disinformation and distort transmitted messages by intruders, including for the purpose of carrying out acts of technical terrorism [3-5]. At the same time, significant complications of situations are possible due to non-objective obtaining of information about the actual state of potentially dangerous objects, as well as the penetration of virus programs into a computer system.

The possibility of carrying out information and psychological operations is also on the agenda, especially during the period of open armed aggression of the Russian Federation against Ukraine. The war in Ukraine showed that the psychological operations units of the armed forces of the Russian Federation are extremely aggressive and capable of exploiting the existing and outdated stereotypes of the population. Psychological operations are actively carried out, which are measures to disseminate specially prepared information in order to influence the emotional state, motivation and validity of actions, decisions made and the behavior of individual leaders and organizations. The computer network Internet has also become a "battlefield", where both sides actively use the network's capabilities for propaganda purposes in order to convey their views on current events to a wide audience.

Due to the fact that the above factors are to be taken into account when monitoring the state of potentially dangerous objects in the conditions of openness of most communication channels, the task of researching, developing and implementing modern methods for ensuring the protection of transmitted information seems to be very relevant.

Analysis of recent research and publications. In a number of works devoted to ensuring the protection of information, as a rule, symmetric cryptographic systems and various methods of control and protection using technical means are considered [6, 7]. The use of symmetric cryptographic systems is associated with the generation, distribution and control of key data, which requires the creation and maintenance of an additional closed system. It should be remembered that the preservation of key data is a paramount concern when using symmetric cryptographic systems. All these factors together imply the creation and maintenance of a very burdensome and rather vulnerable system for generating, storing, controlling and distributing key data.

At the same time, the incompetence and negligence of service personnel is increasingly being used to penetrate computer systems. These shortcomings are absent in cryptographic systems with a public key (asymmetric cryptosystems) [8]. In such systems, one key is used for encryption and another key for decryption. The first key is public and can be published to encrypt their information by any network user. The recipient of the encrypted information uses the second key, which is secret, to decrypt the data. In this case, the condition is met: the secret key cannot be determined from the published public key. However, the algorithms of asymmetric cryptosystems require large computational resources (Table 1).

Table 1 - Comparative characteristics of encryption algorithms

Characteristics of the algorithm	DES, AES, GOST 28147-89	RSA
Encryption speed	High	Low
Encryption function used	Permutation and substitution	Exponentiation
Key length	56 bit	More than 500 bit
The least expensive cryptanalysis (its complexity determines the strength of the algorithm)	Search across the key space	Decomposing a number into prime factors
Key generation time	Milliseconds	Seconds
Key type	Symmetric	Asymmetric

But, due to the huge progress in the field of computer technology, a significant increase in the performance of computer systems of mass personal production, the task of studying the feasibility of introducing asymmetric cryptosystems to improve the information mechanism of state management of monitoring the state of potentially dangerous objects is of particular relevance.

The purpose of the article is to outline the prospects for using asymmetric cryptosystems to improve the information mechanism of state management by monitoring the state of potentially dangerous objects, taking into account modern conditions.

Main Part. To date, Ukraine remains a problem of full integration of subjects of national monitoring into a single system, the development of a single methodology for collecting, accumulating and transmitting monitoring information [9]. Therefore, the legislation defines tasks only for the nationwide monitoring and control system through the collection, processing and transmission of information on the state of the environment, contamination of food products, food raw materials, fodder and water with radioactive and chemical substances, microorganisms and other biological agents [10].

Monitoring is a mechanism that performs systematic monitoring and control of potentially dangerous objects, processes and systems of protection, forecasting zones and consequences of possible emergencies, the state of implementation of preventive measures to reduce their scale, collection, processing, transmission and storage of this information, is monitoring (Fig. 1). It is the information about the state of potentially dangerous objects that circulate in systems for monitoring the state of potentially dangerous objects that needs to be protected in the first place.

The main tools for the implementation of such monitoring are the certification of potentially hazardous objects, declaring the safety of high-risk facilities, expert assessments of the state of readiness of economic facilities and territories for actions to protect and function in emergency situations, a comprehensive assessment to determine the integral indicators of the danger of regions in the event of emergency situations, management a network of observation and laboratory control during a special period (hydrometeorological and sanitary-epidemiological stations, veterinary and agrochemical laboratories). The economic effect of monitoring the state of potentially dangerous objects is obtained by reducing the time for preparing response and liquidation of their consequences, as well as by obtaining objective data for planning.

A unified information environment for the operational supply of such monitoring data to performers in order to predict the risks of occurrence and development of emergency scenarios should be provided by the Government Information and Analytical System for Emergency Situations [11], created to support the processes of preparing, adopting and monitoring the implementation of management decisions related to emergencies, based on the complex processing of operational, analytical, reference, expert and statistical data from various sources (Fig. 1).

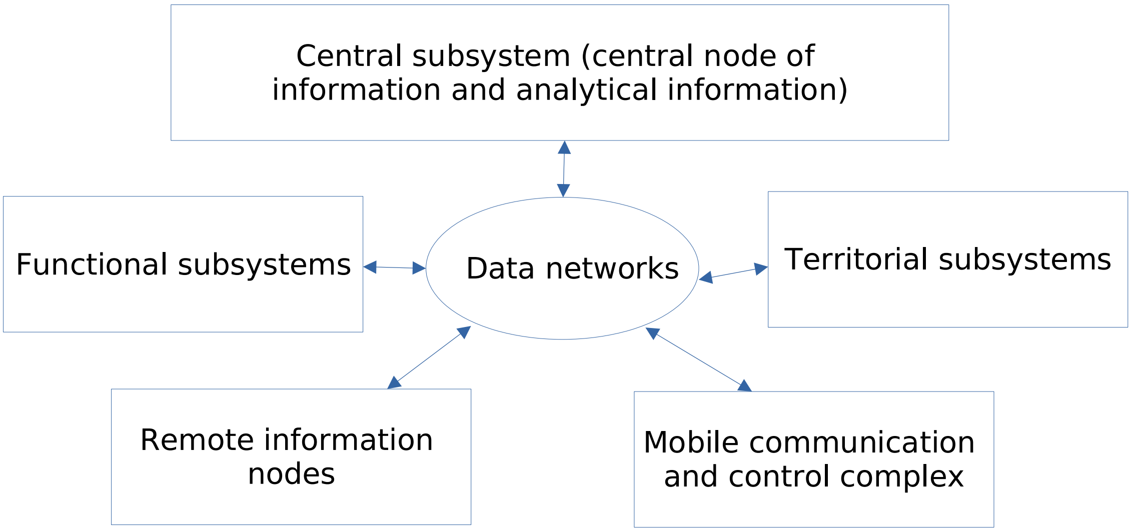
Central subsystem (central node of information and analytical information)
Functional subsystems
Data networks
Territorial subsystems
Remote information nodes
Mobile communication and control complex

Figure 1 - Governmental information and analytical system for emergency situations

Source: compiled on the basis of the Decree of the Cabinet of Ministers of Ukraine dated 12/16/1999 No. 2303 “On the creation of the Governmental information and analytical system for emergency situations” [11]

Obviously, the automation of the processes of obtaining reliable information about the state of potentially dangerous objects and emergencies requires the introduction of cryptographic information protection systems.

To conduct research, the algorithm of the most famous RSA asymmetric encryption system (the name of the algorithm is taken from the first letters of the names of its authors - Rivest, Shamir and Aldeman) was presented as:

1. Two very large primes p and q are randomly chosen;
2. Two factors are calculated n = p x q and m = (p - 1) x (q - 1);
3. A random integer E is chosen, which has no common factors with m;
4. Find D such that DE = 1 modulo m;
5. The original text, X, is divided into blocks so that 0 < X < n;
6. To encrypt a message, it is necessary to calculate C = XE modulo n;
7. For decryption, X = CD modulo n is calculated.

In a system built on the basis of the RSA protocol, anyone who knows the public key can encrypt a message, and only the addressee who has the private key can reveal it. Another property of the RSA protocol is that if you swap the numbers E and D, it turns out that you can encrypt with a private key, and decrypt with a public one. Thus, the sender can encrypt the message, and any recipient can decrypt it. This property forms the so-called "digital signature" [8]. It determines the authorship of the message.

The above property of the RSA algorithm was applied in the development of a research prototype of the program for generating an electronic digital signature (EDS). In order to control the reliability of messages, the convolution property was used (the dependence of the integrity of the message on the key and the generated electronic signature). To transmit a message, a public key and an EDS, it is possible to use conventional communication channels (at the first stage of testing, the transmission was carried out via a local computer network). It is also possible to send a "signed" message through the computer network Internet.

When testing a research prototype of the EDS generation program, in which the dependence of the EDS generation time on the message volume was experimentally determined, it was found that with a text volume of up to 50 pages, the program operation time does not exceed 6 seconds. The experiments were carried out with the following parameters that affect the performance of a computer system: Intel® Pentium® 2117U processor, 2 MB cache, processor operating frequency - 1.8 GHz, RAM - 4 GB, operating system - Windows 10. At the same time, the software the product was developed in the Delphi object-oriented programming environment, has a user-friendly interface and does not require long training. The disadvantages of the research prototype of the EDS generation program include the presence of the EDS itself during the transmission of messages.

The EDS itself is slightly larger than the transmitted message. However, it is this additional file that allows you to confirm the accuracy of the transmitted information.

The Code of Civil Protection of Ukraine determines the need for constant monitoring and forecasting of emergency situations in order to prevent them. The large-scale humanitarian crisis and the destruction of potentially dangerous objects in almost all regions of Ukraine as a result of full-scale hostilities revealed certain shortcomings in the functioning of data transmission systems when monitoring the state of potentially dangerous objects. For Ukraine, the problem remains the full integration of subjects of national monitoring into a single system, the development of a single methodology for collecting, accumulating and transmitting monitoring information [12, 13].

It should be noted that in accordance with the order of the Head of the State Emergency Service of Ukraine “On approval of the Procedure for the use of information and information and telecommunication systems and the Procedure for the use and accounting of computer programs” [14], in the system of emergency situations of Ukraine, priority is given to the use of computer programs for free use. Therefore, the development of specialized software for the implementation of EDS will allow not to purchase expensive software implementations of EDS.

Conclusions and prospects for further research in this direction. Obviously, for the reliable functioning of modern information systems for the transmission of monitoring information about the state of potentially dangerous objects, it is necessary, first of all, to develop highly efficient systems for protecting transmitted data, including asymmetric cryptographic protection systems. The use of EDS in monitoring the state of potentially dangerous objects can significantly increase the reliability of message transmission. Improving the information mechanism of state management of monitoring the state of potentially dangerous objects through the development of software systems based on the functioning of the EDS will allow avoiding information and psychological operations, especially during the period of open armed aggression of the Russian Federation against Ukraine.

The presented research prototype of the EDS generation program allows you to create an EDS for each message separately and allows you to solve the problems of checking the integrity and authenticity of the message, and also does not allow you to introduce misinformation. A feature of this implementation is that all the tasks of protecting and maintaining the integrity of information are solved without the use of encryption equipment. The generation of key data is carried out by means of a PC, and the use of modern asymmetric cryptographic systems makes it possible to send key data through open communication channels.

The conducted studies allow us to say that the use of asymmetric cryptosystems to improve the information mechanism of state management by monitoring the state of potentially dangerous objects is currently promising and justified.

References

1. Kropotov P. P., Bygun V. V., Grechaninov V. F. Creating a modern security monitoring system is an urgent state and scientific task. Information processing systems. 2015. Issue 11 (136). pp. 199–206.

2. Grechaninov V. F. Recommendations regarding the functioning of the unified state system of civil protection in modern conditions (first edition) / Ukrainian Research Institute of Civil Protection. 2016. URL: http://undicz.dsns.gov.ua/files/2016/8/30/Persha_redakciya_rekomendaciy_EDSCZ.pdf

3. Cyber Terrorism and Critical Infrastructure Protection / FBI – The Federal Bureau of Investigation. – URL: http://www.fbi.gov/news/testimony/cyber-terrorism-and-critical-infrastructure-protection

4. Verton, D. Black Ice: The Invisible Threat of Cyber-Terrorism / D. Verton. – N. Y. : McGraw-Hill Osborne Media, 2003. – 273 p.

5. Denning, D. E. Is Cyber Terror next? / D. E. Denning // SSRC – Social

Science Research Council. – URL: http://essays.ssrc.org/sept11/essays/denning.htm

6. J. Daemen, V. Rijmen. The design of Rijndael. AES –The Advanced Encryption Standard. Springer-Verlag, Berlin, 2002.

7. N.T.Courtois, J. Pieprzyk. Cryptanalysis of block ciphers with overdefined systems of equations. Proceedings of Asiacrypt'02, LNCS. Springer-Verlag, Berlin, 2002.

8. 8. Horbenko Y.I., Horbenko I.D. Public key infrastructures. EDS systems. Theory and practice. Kharkiv. - Fort, 2010. - 593 p.

9. 9. Shvedun V. O., Ignatiev O. M. Improvement of state management of monitoring of potentially dangerous objects using the European procedure for assessing the impact on the environment // Adaptation of the legal system of Ukraine to the law of the European Union: theoretical and practical aspects (Poltava, October 22, 2020): in the 2nd part. Poltava: Rossava, 2020. P. 140–142.

10. On the implementation of the Observation Methodology for the assessment of the radiation and chemical situation: Order of the Ministry of Internal Affairs of Ukraine dated November 27, 2019 No. 986 // Database "Legislation of Ukraine" / Verkhovna Rada of Ukraine. URL: https://zakon.rada.gov.ua/laws/show/z0083-20#Text (date of application: 11/22/2021).

11. On the creation of the Governmental Information and Analytical System for Emergency Situations: Decree of the Cabinet of Ministers of Ukraine dated 12.16.1999 No. 2303 // Database "Legislation of Ukraine" / Verkhovna Rada of Ukraine. URL: http://zakon.rada.gov.ua/laws/show/2303-99-%D0%BF (date of application: 11/19/2021).

12. Ihnatiev O. State and problems of the information mechanism of public management of monitoring of the state of potentially dangerous objects in Ukraine. Public administration and state security aspects. 2022. Vol. 2/1. P. 138–149. DOI: 10.52363/passa-2022.1-14.

13. Ignatiev O. M. Analysis and assessment of the organizational mechanism for ensuring state management by monitoring the state of potentially dangerous objects. Law and public administration: coll. of science works 2020. Issue No. 3. P. 100–106. DOI URL: https://doi.org/10.32840/pdu.2020.3.15.

14. On the approval of the Procedure for the use of information and information and telecommunication systems and the Procedure for the use and accounting of computer programs: order of the Head of the State Emergency Service of Ukraine dated 07.19.2019 No. 425. Kyiv: State Emergency Service of Ukraine, 2019.