Journal of Computer Networks, 2014, Vol. 2, No. 2, 23-25
Available online at http://pubs.sciepub.com/jcn/2/2/4

DOI:10.12691/jcn-2-2-4

Information Security of Kazakh Airlines

Zhangisina G.[1,*], Mukanov K.[2], Kuldeev E.[2], Usen A.[3], Pavlikov R.[4]

[1]Honored Worker of Education of Kazakhstan, Head. Department "Information Security" KazNTU named after K.I. Satpaeva, Kazakhstan, Almaty
[2]Vice-rector KazNTU named after K.I. Satpaeva, Kazakhstan,Almaty
[3]Master 1st year degree the Type the (protection and information security), KazNTU named after K.I. Satpaeva
[4]Master 2st year degree the Type the (protection and information security), KazNTU named after K.I. Satpaeva
*Corresponding author: gul_zhd@mail.ru

Received May 30, 2014; Revised June 02, 2014; Accepted June 03, 2014

Abstract In this paper the problems in aviation and Information security of Kazakh airlines are considered. The problems of security in aviation and the principles of safe upper systems for civil aviation enterprises.

Keywords: *protection, security, aviation, system, information*

Cite This Article: Zhangisina G., Mukanov K., Kuldeev E., Usen A., and Pavlikov R., "Information Security of Kazakh Airlines." *Journal of Computer Networks*, vol. 2, no. 2 (2014): 23-25. doi: 10.12691/jcn-2-2-4.

1. Introduction

The law "On the Concept of Information Security of the Republic of Kazakhstan", defining the rules according to which the information relates to confidential, and sets goals of information security:

- Prevention of leakage, theft, misrepresentation, falsification of information;
- Prevent unauthorized actions of destruction, mutilation, blockade;
- Preservation of state secrets, the confidentiality of documentary information.

Information security has three main components: confidentiality (protection of confidential information from unauthorized disclosure), integrity (ensuring the accuracy and completeness of the information and software), accessibility (accessibility of information and vital services for users when required).

But the main goal of information security is to prevent damage to its operations due to the disclosure, leakage and unauthorized access to data sources containing information enclosed.

Information security system

A separate section of the bill "On Commercial Secrets" on the organization of protection of commercial information, defines a set of measures necessary to protect it:

- Establishment of a special regime of confidentiality;
- Limiting access to confidential information;
- Monitoring compliance with the established regime of confidentiality.

Establishment of a special privacy mode aimed at creating conditions for the physical media protection of confidential information. As a rule, special privacy mode implies:

- Organization of protection of the premises, which contain media of confidential information;
- Establishment of a regime of work in areas that contain confidential information media;
- The establishment of access control to premises containing media of confidential information;
- Fastening hardware handling confidential information on employees, the definition of personal responsibility for their safety;
- Establishing procedures for the use of confidential information carriers (accounting, storage, transfer to other officials, destruction, reporting);
- Organization of repair of technical equipment for handling confidential information;
- Organization of control over the established order.

Requirement to establish a special regime in the enterprise policy issued in the form of organizational and administrative documents and communicated for information to employees.

Restricting access to confidential information helps to create the most effective conditions is confidential information. Should clearly define the scope of employees admitted to confidential information to which specific information they are allowed to access and authority staff access to confidential information.

As practice shows the work necessary to develop a set of measures for the protection of information, it is desirable to attract qualified experts in the field of information security.

Traditionally, the organization of access to confidential information used organizational measures based on strict adherence to procedures for the approval employees to information determined appropriate instructions, orders and other regulatory documents. However, with the development of computer systems, these measures have ceased to provide the necessary security information. There are currently and widely used specialized software and firmware information security that allow to automate the procedures for access to information and thus provide the required degree of protection. More about the existence of information security discussed below.

Monitoring compliance with established privacy mode provides verification of compliance information security organization established requirements, as well as evaluating the effectiveness of measures to protect information. Typically, the control is carried out as scheduled and unscheduled inspections with its own employees or with the assistance of other organizations that specialize in this area. The results of checks on data protection experts conducted the necessary analysis to the preparation of the report, which includes:

- Conclude that the activities conducted by the company with the requirements;
- Evaluation of the real effectiveness of enterprise information security measures and proposals for their improvement.

Provision and implementation of the above activities will require the establishment of appropriate bodies in the enterprise data protection. Effectiveness of information security in the enterprise will be largely determined by how properly selected body structure to protect information and its employees are qualified. Typically, the information security bodies are independent units, but in practice often practiced and the appointment of one of the professional staff of the enterprise responsible for ensuring the protection of information. However, this form is justified in cases where the amount of the necessary measures for the protection of information and the creation of a small separate unit is not economically viable.

Requirements for information security airlines

The main requirements for information security firm are:

- Protection of information containing information covered;
- Organization of the legal, organizational and engineering (physical, hardware, software and mathematical) Protection of information containing information covered;
- Organization of a special office, exclusive steal information containing information covered;
- Preventing unjustified admission and access to information, information containing closed;
- The identification and localization of possible leakage channels classified information in the course of daily production activities and in extreme (emergency, fire, etc.) situations;
- Ensuring the security of information in all types of activities, including a variety of meetings, negotiations, meetings related to business cooperation, both at the national and international level;
- Ensuring the protection of buildings, facilities, equipment, products and technical means of information security;
- Private security officers and leading experts and staff;
- Assessment of marketing situations and misconduct intruders and competitors.

General functions of information security:

- Organizes and provides throughput and intrabuilding regime in buildings and premises, the order of service protection, monitors compliance regime employees;
- Directs the work on the legal and institutional regulation of relations for the protection of classified information;
- Participates in the development of basic documents in order to consolidate their requirements for security and protection of classified information;
- Develop and implement together with other departments to ensure the event with documents containing sensitive information, for all kinds of work, organizes and supervises the compliance regulations on the protection of information containing information covered;
- Examines all aspects of industrial, commercial, financial and other activities to identify and close possible leakage channels classified information;
- Organizes and conducts official investigation into the disclosure of classified information;
- Develop, maintain, update and add to the list of information containing the information enclosed, and other regulations governing the security and protection of information;
- Ensures strict compliance regulations to protect information;
- Manages the departments and divisions airline security to protect information;
- Organizes and regularly conducts training of security personnel in all areas of information security, ensuring that the protection of private information was deeply conscious approach;
- Keeps records safes, metal cabinets, storage and other special spaces where permitted permanent or temporary storage of classified information;
- Keeps records allocated for confidential work premises, means they have the potential of information leakage.

Security officers airlines in order to protect private information, have the right to:

- Require all employees strictly and scrupulously comply with regulations or contractual obligations to protect private information;
- Make proposals to improve the legal, organizational and technical activities for the protection of information.

Required to:

- Monitor compliance with regulations on the protection of information;
- Management report on violations of regulatory requirements for the protection of information and other actions that could lead to leakage of confidential information, or loss of documents;
- Prevent unauthorized access to documents and materials containing closed information to unauthorized persons.

Security officers are responsible for airline security breach private information containing information and closed for non-fulfillment of their rights at the functional responsibilities for the protection of classified information enterprise employees.

Means or instruments by which is possible to achieve the objectives of information security.

We list the main means (tools) Information Security:

- staff - the people who will ensure the implementation of information security in all aspects, that is, to develop, implement, maintain, monitor, and execute;
- regulatory support - the documents that create legal prospace for the operation of information security;
- security model - providing information security schemes STI inherent in this particular information system or environment;
- cryptography - methods and tools for converting the information into the form, making it difficult or impossible for unauthorized transactions with it (read and / or modification), together with the methods and means of

creating, storing and distributing keys - special information objects that implement these sanctions (symmetrical / asymmetrical, in-line / block encryption);

- antivirus software - a means to detect and eliminate malicious code (viruses, Trojans, etc.);

- firewalls - device access control information from one network to another;

- security scanners - devices functioning quality assurance security model for this particular information system;

Intrusion Detection Systems - devices for monitoring activity in the information environment, sometimes with the ability to make independent participation in this vigorous activity;

- backup - save redundant copies of information resources in the event of possible loss or injury;

- duplication (redundancy) - the creation of alternative devices of necessary for the functioning of the information environment, designed for chennyh cases of failure of the main device;

- emergency (crisis) plan - a set of activities designed to implement, if events occur or did not occur as was predetermined rules of information security;

- user training - training active participants information tional environment for working in compliance information security.

Organizational and technical measures to protect information

Security system should be:

- Centralized - ensuring effective control of the system from the head and officials responsible for the various activities of the company;

- Planned - uniting the efforts of various officials and structural units to carry out the tasks facing the company in the field of information security;

- Specific and focused - is designed to protect specific information resources of interest to competing organizations;

- Active - protects information with sufficient perseverance and the ability to focus on the most important areas of the enterprise;

- Reliable and versatile - covering all activities of the company associated with the creation and exchange of information.

There are certain rules which it is advisable to stick to the organization of information security:

- Establishment and operation of security systems is a difficult and responsible task. Do not trust the protection of information amateurs, instruct them to professionals;

- Do not try to organize an absolutely reliable protection - this simply does not exist. Protection system must be sufficient, reliable, efficient and manageable. Effectiveness of information security is achieved not by the quantity of money spent on its organization, and its ability to adequately respond to all attempts of unauthorized access to information;

- Measures to protect the information from unauthorized access must be comprehensive in nature, ie combine disparate measures countering threats (legal, organizational, technical and software);

- The main threat to information security of computer systems comes directly from employees. With this in mind, it is necessary to limit the maximum range as employees admitted to confidential information, and the range of information to which they were admitted (including the Information Protection System). In addition, each employee must have a minimum of powers of access to confidential information.

An integrated approach to the development stage protection system to avoid unnecessary expenditure of time and resources in creating an integrated enterprise security.

Naturally, an integrated security system requires a significant investment. However, if you carefully evaluate all of the negative factors that affect the activity of the enterprise, these costs do not seem as big as they provide sustainable economic development of the company and minimize possible losses.

In addition, the process of creating an integrated security system can be extended in time taking into account the financial possibilities of the enterprise and the conditions of its activity in the market.

2. Conclusion

In this paper the problems in aviation and Information security of Kazakh airlines were considered.

References

[1] Zhangisina G.D. The cost-effectiveness of information security system. International Conference. Bulgaria 2011.

[2] Zhangisina G.D. Information security system. International Conference. Czech Republic, 2011.

[3] Zhangisina G.D., Usen A. Tursynova M., D. Akhmetov problem of information security. Search, 2013. № 2 (1).

[4] Zhangisina G.D., Rysty OM Pavlikov R., Usen, A., D. Akhmetov, Berkimbaeva A. On the methods and means of protection against leakage of information through technical channels. Search, 2013. № 1 (1).

[5] Zhangisina G.D., Shayhanova AK Rystaev O., D. Akhmetov, Tursynova M. Ombaev NO The problem of data security in organizations and enterprises. Search, 2013. № 2 (1).

[6] PB Horev Methods and tools for information security in computer systems. Moscow: Academy, 2005.