**International Journal of Academic and Applied Research (IJAAR)**
**ISSN: 2643-9603**
**Vol. 5 Issue 1, January - 2021, Pages: 58-61**

# Physical Security

**Usmonov Makhsud**

Tashkent University of Information Technologies, Karshi branch 3rd year student
+99891 947 13 40
***maqsudusmonov22@gmail.com***

**Abstract:** The purpose of a system of physical protection of information sources is to prevent the intruder from infiltrating the protected information sources and to warn of natural disasters, primarily fire. Engineering constructions create barriers that prevent the spread of threats to information sources. The uncertainty of the types and timing of threats to information, the number and variety of means of protecting information, and the lack of time in emergencies place high demands on the management of physical means of information protection.

**Keywords:** Engineering protection and technical protection of objects, system of physical protection of information sources, Autonomous protection system.

## INTRODUCTION

1. System of physical protection of information sources

2. Engineer protection of information

The purpose of the physical protection system is to prevent the intruder from infiltrating the protected information sources and to warn of natural disasters, especially fire.

Engineering constructions create barriers that prevent the spread of threats to information sources.

The uncertainty of the types and timing of threats to information, the number and variety of means of protecting information, and the lack of time in emergencies place high demands on the management of physical means of information protection.

Management should ensure that:

• Implementation of general principles of information protection;

• Coordination of the physical protection system of information and its leakage protection system in a single framework;

• make operational decisions on information security;

• Monitoring the effectiveness of safeguards.

## METHODS

Regulations for the management of physical protection systems are set out in information security guidelines. However, the guidelines do not cover all situations. The means of the physical defense system must ensure that the correct conclusions are drawn in the event of atypical situations in the context of time constraints.

The structure of the physical protection system is diverse: from a simple locked wooden door to an automated security system. A generalized schematic of the physical protection system is shown in Figure 7.

The need for engineering protection and technical protection of facilities is confirmed by statistics, that is, if more than 50% of infiltration is carried out by employees and customers on freely accessible facilities, only 5% of strong security regime weather ect.

Figure 16.1. The structure of the system of physical protection of the information source

Information security is provided by the following:

• Natural and man-made roadblocks that may interfere with the information (or valuables) of the intruder and the disaster;

• Blocking devices for control and management systems.

Natural barriers include areas (ditches, ravines, cliffs, rivers, dense forests, and forests) that are difficult to walk on or near the organization, and should be used to strengthen boundaries.

Artificial barriers are man-made and differ significantly from natural barriers in their design and resistance to destructive influences. They include various walls, floors, ceilings, building windows, and so on. relevant

The windows are reinforced with mechanical glass and metal bars.

The final boundaries of protection are metal cabinets, safes. Therefore, high demands are placed on their mechanical strength.

Metal lockers are designed to store documents, valuables, and small amounts of money that are not highly classified. The reliability of the cabinets depends only on the strength of the metal and the secrecy of the locks.

Figure 16.2 shows a typical structure of a complex of technical means of protection of objects. A sensor is a technical device that generates an alarm signal when it is subjected to mechanical force and field by an intruder.

The alarm loop forms an electrical circuit that provides electrical connection to the sensors and receiver-control devices.

The receiver-control point is designed to receive and process signals from the sensors, to inform security personnel about the arrival of alarm signals using sound and light signals, malfunctions of sensors and plumes.

Figure 16.2. Model structure of a complex of technical means of protection of objects

Television surveillance systems are now widely used. The system also includes on-duty lighting devices that provide the required level of illumination in the protected area at night .

The operation of an autonomous security system is costly. For this reason, centralized security systems are widely used. In this system, the issue of neutralizing intentional violations is common to several organizations.

Examples of centralized security are savings bank branches, small firms, private houses, country houses, and apartments.

## RESULTS

Natural barriers include areas (ditches, ravines, cliffs, rivers, dense forests, and forests) that are difficult to walk on or near the organization, and should be used to strengthen boundaries.

Artificial barriers are man-made and differ significantly from natural barriers in their design and resistance to destructive influences. They include various walls, floors, ceilings, building windows, and so on. relevant

The windows are reinforced with mechanical glass and metal bars.

The final boundaries of protection are metal cabinets, safes. Therefore, high demands are placed on their mechanical strength.

Metal lockers are designed to store documents, valuables, and small amounts of money that are not highly classified. The reliability of the cabinets depends only on the strength of the metal and the secrecy of the locks.

Figure 16.2 shows a typical structure of a complex of technical means of protection of objects. A sensor is a technical device that generates an alarm signal when it is subjected to mechanical force and field by an intruder.

The alarm loop forms an electrical circuit that provides electrical connection to the sensors and receiver-control devices.

The receiver-control point is designed to receive and process signals from the sensors, to inform security personnel about the arrival of alarm signals using sound and light signals, malfunctions of sensors and plumes.

Figure 16.2. Model structure of a complex of technical means of protection of objects

Television surveillance systems are now widely used. The system also includes on-duty lighting devices that provide the required level of illumination in the protected area at night .

The operation of an autonomous security system is costly. For this reason, centralized security systems are widely used. In this system, the issue of neutralizing intentional violations is common to several organizations.

## DISCUSSION

The need for engineering protection and technical protection of facilities is confirmed by statistics, that is, if more than 50% of infiltration is carried out by employees and customers on freely accessible facilities, only 5% of strong security regime weather ect.

Figure 16.1. The structure of the system of physical protection of the information source

Information security is provided by the following:

• Natural and man-made roadblocks that may interfere with the information (or valuables) of the intruder and the disaster;

• Blocking devices for control and management systems.

Natural barriers include areas (ditches, ravines, cliffs, rivers, dense forests, and forests) that are difficult to walk on or near the organization, and should be used to strengthen boundaries.

Artificial barriers are man-made and differ significantly from natural barriers in their design and resistance to destructive influences. They include various walls, floors, ceilings, building windows, and so on. relevant

The windows are reinforced with mechanical glass and metal bars.

The final boundaries of protection are metal cabinets, safes. Therefore, high demands are placed on their mechanical strength.

## CONCLUSION

The purpose of the physical protection system is to prevent the intruder from infiltrating the protected information sources and to warn of natural disasters, especially fire.

Engineering constructions create barriers that prevent the spread of threats to information sources.

The uncertainty of the types and timing of threats to information, the number and variety of means of protecting information, and the lack of time in emergencies place high demands on the management of physical means of information protection.

## REFERENCES

1 Seymour Bosworth, Michel E. Kabay, Eric Whyne. Computer security handbook. Wiley.2014.

2 Bulletin of the Oliy Majlis of the Republic of Uzbekistan. - T., 2003. - №1. - 2-m.

3Information security in the field of communication and information: Terms and definitions. Network standard: TSt 45-010: 2010.

5 Bulletin of the Supreme Council of the Republic of Uzbekistan. - T., 1993. - №5. - 232-m.

6 Sean Harris. ALL IN ONE CISSP. McGraw-Hill. 2013.

7 Explanatory dictionary of information and communication technologies (second edition). - T., 2010.

8 See Tadjikhanov B.U. Ugolovno-pravovye mery borby s terrorizmom / Otv. ed. Ph.D. jurid. nauk A.S. Yakubov. - T .:, 2003. - S.4–20; Naumov A.V. Rossiyskoe ugolovnoe pravo. Obshchaya chast. - M., 1999. –162–163.

9 See Krylov V. Informatsionnye prestupleniya - novyy kriminologicheskiy object // Rossiyskaya yustitsiya. - 1997. - № 7 - S.22 - 23.

10 See Chichko L.. Kompyuternye xishcheniya // Rossiyskaya yustitsiya. - 1996. - №5. - S.45.

11 See Vexov V.B. Computer prestupleniya: sposoby sovershenіya i raskrytiya. - M., 1996. –S.163.

12 See Sorokin A.V. Computer prestupleniya: ugolovno-pravovaya characteristics, metodika i praktika raskrytiya i rassledovaniya. Internet resource: //http://kurgan.unets.ru/~procur/my_page.htm, 1999.

13 See Ugolovnoe pravo. Special time. - M., 1998. - S.546.

14 See Ugolovnoe pravo. Obshchaya chast / A.S.Yakubov, R. Kabulov et al. - T., 2005. - p. 112-119.

15 See Krylov V.V. Informatsionnye kompyuternye prestupleniya: Uchebnoe i prakticheskoe posobie. - M., 1997. - p. 40-44; Bogomolov M.V. Ugolovnaya otvetstvennost za nepravomernыy dostup k oxranyaemoy zakonom kompyuternoy informatsii. - Krasnoyarsk, 202. - S, 8 - 14; 62-64.

16 See Sottiev I.A. Legal means of combating organized crime: Textbook - T, 2005. - pp. 30-43.