Tomasz Kośmider[1]
Jerzy Trocha[2]

Prawny oraz praktyczny wymiar ochrony obszarów, obiektów i urządzeń istotnych dla bezpieczeństwa państwa

DOI: 10.5604/01.3001.0015.5416

Streszczenie

W artykule zostały omówione prawne zobowiązania kierowników jednostek znajdujących się w ewidencji obszarów, obiektów i urządzeń podlegających ochronie. Realizacja tego zadania wymaga współpracy i współdziałania służb, straży i inspekcji z sektorem prywatnym, stanowiąc warunek *sine qua non* budowania pożądanego poziomu bezpieczeństwa. Idea zapewnienia fizycznej lub technicznej ochrony obiektu o istotnym znaczeniu dla bezpieczeństwa państwa, uwzględniająca wykorzystanie wewnętrznych służb ochrony bądź agencji ochrony osób i mienia, nie ma jednoznacznych ocen.

Ponadto zostały zaprezentowane praktyczne sposoby zapewnienia bezpieczeństwa obszarów, obiektów i urządzeń podlegających obowiązkowej ochronie. Obecny rozwój technologiczny nie sprowadza ochrony obiektu wyłącznie do ochrony fizycznej, umożliwiając wykorzystanie nowoczesnych systemów zabezpieczenia technicznego celem wsparcia działań pracowników specjalistycznych uzbrojonych formacji ochronnych. Z uwagi na powyższe autorzy przedstawili działanie wybranych systemów zabezpieczenia technicznego w obiektach chronionych.

Słowa kluczowe: bezpieczeństwo, ochrona, prawo, obiekt, kontrola dostępu, monitoring

[1] Professor of social sciences (security sciences), director of the Institute of Security Sciences of the Academy of Justice, in 2012-2018 director of the Institute of State Security of the National Defence University of Warsaw/the War Studies University.
ORCID ID: 0000-0003-2129-3642.

[2] Doctor of security sciences, assistant professor at the Academy of Justice, specialist in technical safeguards and physical security in public and private sector enterprises. ORCID ID: 0000-0002-2561-4485.

Legal and practical dimensions of the protection of areas, facilities and devices important for state security

Abstract

The article discusses the legal obligations of heads of units included in the register of areas, facilities and devices subject to mandatory protection in the voivodeship. The obligation of the head of the unit to provide physical or technical protection of an object. Significant items for state security with the use of internal security services or personal and property protection agencies – that is often criticised. However, it should be remembered that the cooperation of services, guards and inspections with the private sector is necessary to obtain the appropriate level of security.

In addition, practical ways to ensure the safety of areas, facilities and devices subject to mandatory protection are also presented. The current technological development does not reduce the protection of the facility only to physical protection, allowing the use of modern technical security systems in order to support the activities of specialised employees of armed security formations. Due to the above, the authors described the operation of selected technical security systems in protected facilities.

Keywords: safety, security, law, facility, access control, video surveillance

1. Introduction

Coping with modern threats concerning the dimension of both structural and personal safety depends to a great extent on the effectiveness of operations of security entities – specialised in performing diverse tasks – whose purpose is to ensure public security and order, proper protection of property and human health, as well as creation of conditions conducive to the economic development of the country[3]. Facilities of key importance for the functioning of the state take a special place in this scope of operations. For this reason, issues related to counteracting their potential threats was regulated legally in the Polish Act of 22 August 1997 on protection of persons and property, pursuant to which competences related to the protection of essential areas, facilities and devices were entrusted to internal security services and personal and property protection agencies. This solution is unprecedented as earlier the liability for the issue of such key importance from the point of view of the state security has never been delegated to commercial security entities. Operations in this scope are focused on physical and technical protection. Details related to ensuring the security of an area, facility or device subject to mandatory protection depend on the type of the activity for which they are intended, their size and the threat level. Managers of units subject to mandatory protection play an essential role in this process in accordance with the provisions of the above-mentioned Act on protection of persons and property.

The proper level of security of areas, facilities and devices subject to mandatory protection – constituting a serious challenge – enforces the necessity to have and continuously improve a system enabling appropriate reactions to threats in the public space. Bearing in mind such a defined purpose of research, the authors have formulated the research hypothesis constituting the assumption that the practical way to ensure safety of the above-mentioned areas, facilities and devices consists in the synchronous use of physical protection and technical security systems. In the course of solving research problems, the authors have applied the analytical and critical method allowing them to achieve the assumed purpose of research and to verify the adopted research hypothesis.

[3] T. Kośmider, *Determinants of the process of creating national security,* 'Journal of Security and Sustainability Issues', 2021, no. 11, p. 287-289.

2. Obligations of managers of units subject to mandatory protection

A manager of a unit (facility owner, administrator or manger, as well as liquidator or receiver) managing a business entity, enterprise, areas or facilities has the right to perform activities aimed at: preventing the occurrence of crimes and offences in relation to the property possessed, preventing unauthorised persons from entering the managed area as well as increasing the level of security and providing personal inviolability to all persons within the managed area.

In the case of areas, facilities and devices subject to mandatory protection, this right is an obligation regulated in the Polish Act of 22 August 1997 on protection of persons and property. Failure to ensure physical or technical protection by the unit manager may lead to the imposition of a penalty in the form of a fine, restriction of liberty or imprisonment even up to 2 years[4].

Registers of areas, facilities and devices subject to mandatory protection within the territory of a province are maintained by province governors and are of a confidential nature[5]. Entering a given facility into the list requires an administrative decision, and the unit manager is obliged to ensure security with the use of specialised armed security formations or technical protection[6].

The legislator has classified areas, facilities and devices important from the point of view of the functioning of the state and its defence, subject to mandatory protection. The catalogue developed contains the following entities:

- special production plants, plants conducting scientific-research or construction works in the scope of such production, plants producing, renovating and storing military weapons and equipment, as well as warehouses of strategic reserves referred to in Article 15 of the Polish Act on strategic reserves[7];
- seaports and airports, entities liable for producing, storing or transporting cash of a significant value, plants related to the extraction of mineral resources of strategic importance for the state;
- plants, facilities and devices of significant importance for the functioning of urban agglomerations, mainly power and heating plants, water intakes, water supply and sewage treatment plants, as well as devices located in an open area, such as fuel pipelines, power and telecommunications lines, dams and sluices, whose destruction or damage may pose a threat to human life or health or the environment, plants using, producing or storing large quantities of radioactive materials, sources and their waste, toxic, intoxicating, explosive and chemical materials of high susceptibility to fire and explosions;
- state archives, facilities storing cultural goods, telecommunications, postal, television and radio facilities and devices, as well as plants with unique economic production;
- construction facilities, systems, devices and services included in a uniform list of systems, devices and services forming critical infrastructure[8].

These facilities are protected according to the adopted algorithm included in the protection plan

4 Polish Act of 22 August 1997 on protection of persons and property (Journal of Laws of 1997, no. 114, item 740, Article 48).

5 *Ibidem,* Article 5(5).

6 *Ibidem,* Article 5(1).

7 Polish Act of 29 October 2010 on strategic reserves (Journal of Laws of 2017, item 1846 and of 2020, item 374).

8 Polish Act of 22 August 1997 on protection of persons and property, Article 5(2).

agreed with the territorially competent Provincial Police Commander, and in the scope of terrorist threats with the director of the branch office of the Internal Security Agency. The State Fire Service has not been included in the process of agreeing the plan. It is however worth noting that the protection plan contains issues concerning fire safety, e.g. fire-fighting system, plans of floors with evacuation routes and location of extinguishing agents. The participation of the provincial commander of the State Fire Service in the process of developing the above-mentioned document seems to be absolutely justified.

The manager of the unit included in the register of the province governor or a person authorised by them is liable for agreeing the plan[9]. Despite the legal obligation to ensure safety of areas, facilities and devices subject to mandatory protection imposed on managers of these units, independent operations in this scope are supervised by the Police. Moreover, the legislator has entrusted the supervision over specialised armed security formations to the Commander-in-Chief of the Police. It should be noted that authorisations in this scope, concerning mainly the right to enter the areas and facilities in which the protection is carried out, interfere significantly in activities of personal and property protection agencies with the status of specialised armed security formations[10].

The protection plan is an important document containing information about the unit's activities, the analysis of the state of possible threats and current level of its safety, assessment of the state of protection, data of the specialised armed security formation, technical security measures as well as principles of protecting the facility subject to mandatory protection[11]. Entities authorised to develop the protection plan – in the scope of direct physical protection – include persons entered into the list of qualified physical security officers[12], while in the aspect referring to technical security measures – persons included in the list of qualified technical security officers[13]. Relevant lists are maintained by the Commander-in-Chief of the Police, and the request for entry is submitted through an appropriate provincial commander of the Police after the fulfilment of a number of criteria determined in the above-mentioned Act on protection of persons and property.

The person preparing the protection plan, the unit manager or anther authorised person issues a confidentiality clause for the plan[14]. Common practice used by economic entities is to issue for this type of documents the 'BUSINESS SECRET' clause. It is not forbidden, but significantly reduces the level of securing the protection documentation against access of unauthorised persons. Taking into account the fact that disclosing the protection plan of an area, facility or device subject to mandatory protection may have an adverse impact on the performance of tasks concerning national defence, public security or economic interests of the state, it is justified to apply at least the 'RESTRICTED' clause, especially that it does not depend on possession by the entrepreneur of the industrial security certificate[15]. Nevertheless, while developing the protection plan of an area, facility or device subject to mandatory protection, an

9 *Ibidem,* Article 7(1).

10 G. Gozdór, *Polish Act on protection of persons and property. Commentary* (*Ustawa o ochronie osób i mienia. Komentarz*), Warsaw 2005, p. 231-232.

11 Polish Act of 22 August 1997 on protection of persons and property, Article 7(2).

12 *Ibidem,* Article 26(2)(1).

13 *Ibidem,* Article 27(4)(1).

14 Polish Act of 5 August 2010 on protection of classified information (Journal of Laws of 2010, no. 182, item 1228, Article 6(1)).

15 Pursuant to Article 54(2) of the Polish Act of 5 August 2010 on protection of classified information, an entrepreneur performing an agreement or task related to access to classified information classified as 'CONFIDENTIAL' or above is obliged to have the industrial security certificate.

enterprise should be able to protect classified information. Due to the above, it seems to be reasonable to impose the obligation to have the industrial security certificate on economic entities whose unit managers develop the protection plan.

The protection documentation prepared in two copies(for each of the parties) is agreed with the territorially competent Provincial Police Commander, while only materials referring to the protection and technical security measures are subject to this process. Issues related to fire hazards or malfunction of ICT systems used in the facility fall outside of the Police competences. However, these elements should be included in the protection plan after the consultation with the provincial commander of the State Fire Service. While performing the analysis of the provisions of the protection plan, the Police before consultations may verify their compliance with the facility's actual state. Pursuant to the provisions of the Act, the manager of the unit subject to mandatory protection is to ensure security, using specialised armed security formations (physical protection) or appropriate technical security measures[16].

Practice adopted in the case of developing the protection plan shows that in principle there are no methods using only one of the above forms. The most frequent as well as the most effective way of protection is to combine both these elements. In this case a specialised armed security formation is complemented by systems of technical security measures, increasing the security level. Moreover, security guards present at the facility may verify quickly the alarm signal from a specific place within the facility. There is however a serious problem consisting in the fact that entities subject to protection do not carry out comprehensive and constant modernisation of systems of technical security measures, which is of key importance for maintaining an optimal level of security. The increase in threats, resulting from technological development, causes the risk of decrease in the effectiveness of protection operations performed.

3. Ensuring physical protection

The entry into force of the Polish Act of 22 August 1997 on protection of persons and property imposed the liability for the protection organisation on managers of units of strategic importance for the security of the state and its citizens, relieving at the same time state services, guards and inspections. The physical protection of areas, facilities and devices subject to mandatory protection may be provided only by specialised armed security formations that can have firearms and use means of direct coercion[17]. The following entities are authorised to perform these tasks:

- internal security services, e.g. Airport Security Services, Warsaw Metro Security Services;
- licensed personal and property protection agencies holding the bearer weapon permit;
- cooperation of internal security services with a licensed personal and property protection agency.

Direct physical protection may be carried out in a permanent or temporary form, while the recommended way of the protection of facilities during their working hours is permanent protection. The similar form of protection is recommended in the case of facilities functioning on a 24-hour basis. In the

16 Polish Act of 22 August 1997 on protection of persons and property, Article 5(1).

17 Polish Act of 24 May 2013 on means of direct coercion and firearms (Journal of Laws of 2013, item 628, Article 2(1)(20); T. Kośmider (ed.), *Means of Direct Coercion. Scope and Ways of Use on the Example of Selected Security Entities (Środki przymusu bezpośredniego. Zakres i sposoby użycia na przykładzie wybranych podmiotów bezpieczeństwa),* Warsaw 2020.

vast majority of facilities subject to mandatory protection, external personal and property protection agencies are liable for security. They are employed by private enterprises or chosen by means of an open tender procedure under a public procurement in the case of entities of the public finance sector. The provision of the service in the form of permanent physical protection and the provision of this service by intervention group in a temporary form (by a specialised armed security formation) constitute examples of the performance of physical protection in a facility subject to mandatory protection. Security employees should remain in constant contact by means of radio communication. A shift commander is appointed from employees assigned to the provision of protection services. This commander is liable for:

- planning tasks of subordinate security employees;
- informing the unit manager about the state of threat and facility protection;
- supervising the storage of means of direct coercion and their recording;
- managing employees providing services in the scope of physical protection of persons and property;
- supervising and checking the performance of obligations by security employees.

Additionally, depending on the size of the facility, patrols as well as permanent and temporary posts are established.

Most frequently security patrols are equipped with the following means of direct coercion: handcuffs, police tonfa baton, hand-held disabling gas thrower and objects intended to incapacitate people with the use of electricity with an average value of the current in the circuit not exceeding 10 mA. A specialised armed security formation also has firearms together with ammunition stored in the weapon warehouse fulfilling requirements determined in the Regulation of the Minister of the Interior and Administration of 21 October 2011 on principles of weapons of specialised armed security formations and conditions of storing and recording weapons and ammunition[18].

The service provider is obliged to ensure readiness for immediate action at the premises of the facility of intervention groups able to react quickly to threats. The group should be equipped with firearms and means of direct coercion. In addition to emergency calls and actions undertaken in response to them, adequate to the event occurred, the intervention group may carry out ad hoc inspections of the protected facility in accordance with the service agreement.

4. Selected systems of technical security measures

The diversity of facilities subject to mandatory protection affects methods in which they are secured. It depends on many factors. The most important of them include: type, designation, materials from which the building was constructed and its age – facilities subject to mandatory protection may be entered into the list of the provincial conservator of monuments, which limits the possibility of installing modern systems of technical security measures. In such cases, changes interfering in the architecture of the building require consultation with the provincial conservator of monuments, which prolongs the preparatory process of the

[18] Regulation of the Minister of Internal Affairs and Administration of 21 October 2011 on principles of weapons of specialised armed security formations and conditions of storing and recording weapons and ammunition (Journal of Laws of 2011, no. 245 item 1462, § 8-18).

facility modernisation in terms of security.

Technical security measures constitute the second way of protection provided for in the Polish Act of 22 August 1997 on protection of persons and property. This concept covers with its scope both electronic and mechanical security measures. This form of protection includes 'activities consisting in the installation, operation, maintenance and repairs of electronic devices and mechanical security measures'[19]. It should be outlined that the unit manager may order the performance of design, construction, implementation and commissioning of technical security measures in the facility only to an enterprise holding the concession of the Ministry of the Interior and Administration for conducting business activity in the scope of personal and property protection services in the form of technical security measures[20].

Currently apart from traditional physical protection, the comprehensive protection of facilities subject to mandatory protection uses different systems of technical security measures, including: access control systems, intrusion and assault warning systems, video surveillance systems (CCTV), fire protection systems and dosimetry systems.

These systems support physical security officers, increasing their effectiveness and, at due to this, the level of security of the facility protected. They operate in a preventative manner, addressing threats and allowing effective management of crisis situations.

In facilities where a large number of technical security measures are installed, it is extremely important to integrate them. The need of interoperability between intrusion and assault warning systems, access control systems or CCTV and fire protection systems is also noticed[21]. On the market there are many platforms, which allow collecting, processing and gathering information according to specific safety procedures. Events on a platform integrating systems of technical security measures are classified according to their category and significance, which enables the operator to handle all systems through one platform. Procedures of the integrating system may include the so-called 'actions to be performed' in the case of receiving an alarm. It is possible to assign to each type of event any number of 'actions' which must be performed in the case of receiving a specific message. They are combined with procedures, which may be assigned to one, or more sensors in the case of an alarm, which makes the operator's work much easier[22].

The task of the protection also includes the surveillance of signals from electronic devices and alarm systems. The full scope of obligations in the case of using systems of technical security measures covers also:

- monitoring of areas covered with protection through the integrated security system, including: CCTV, intrusion and assault warning systems, access control systems and other systems as well as operation of these system in order to:

---

19 R. Kręgulec, P. Pajorski, *Polish Act on protection of persons and property. Commentary (Ustawa o ochronie osób i mienia. Komentarz),* Warsaw 2015, Article 3.

20 Pursuant to the decision of the National Appeal Chamber of 28 October 2014, KIO 2094/14, LEX no. 1567433, in the case of publication of tender notice by the owner of the facility subject to mandatory protection for the design, construction, implementation and commissioning of visual monitoring, access, burglary and assault control or radiation measurement, enterprises submitting their bids are not required to have the concession for conducting business activity in the scope of protecting people and property in the form of direct physical protection.

21 A. Misiuk, M. Kalaman, *Directions of Organisational and Technical Changes in the Prison Service (Kierunki zmian organizacyjno-technicznych w Służbie Więziennej),* Warsaw 2016, p. 185.

22 *Ibidem.*

- » identify persons violating order regulations;
- » detect and record such events as crimes, offences, threats to life and health, damage to property as well as to support activities of law enforcement authorities;
- » detect unattended luggage, packages and other items;
- » counteract the presence at the facility of persons violating order regulations;
- » counteract the presence at the protected area of motor vehicles without appropriate authorisations;
- » submit necessary information about detected irregularities to appropriate employees and other authorised entities;

- 24x7 monitoring of threats at the facility and external adjacent areas;
- obtaining, gathering, processing and transferring information from systems of technical security measures functioning in the protected facility;
- cooperation with services, inspections and other public authorities in the scope of exchange of information for the purpose of ensuring security;
- informing relevant services and institutions about events at the facility subject to mandatory protection depending on the character of the event.

4.1. Access Control Systems

The first system of technical security measures commonly applied at facilities subject to mandatory protection is the access control system. It is used to manage persons' authorisations to access specific areas or places at the facility, as well as to identify persons entering premises covered by the system. These persons enter and leave the premises with the use of a 'key' in the form of a magnetic card, biometric feature, numerical code, password or key fob[23]. The use of a traditional key is limited. The system administrator is authorised to grant users access and to revoke it, which is particularly important in the case of locked premises to which many persons have access, as well as in the case of loss of the magnetic card or key fob. In such a situation it is not necessary to replace the door locks, but only to block the lost device for unlocking them.

Access control systems using biometric features present a significantly higher level of security due to limiting the risk of losing the magnetic card or key fob or obtaining the numerical code or password by unauthorised persons[24]. However it involves higher costs of purchasing the system and maintaining its efficiency. An important feature of the access control system is scalability and openness allowing free adjustment of the size of the area covered with the access control. Due to the above, different systems are applied depending on the size of the facility: from facilities with one or two access control points and the group of authorised employees up to 100 persons, to facilities with as many as 10,000 access control points and the group of authorised employees up to 1,000,000 persons. Another important feature of the

[23] R. Ćwirko, J. Ćwirko, *Modular Access Control System for Teaching Purposes (Modułowy system kontroli dostępu dla dydaktyki),* 'Measurements. Automation. Control' (Pomiary. Automatyka. Kontrola) 2014, 60, no. 9, p. 756.

[24] T. Dąbrowski, M. Bednarek, M. Wiśnios, *Method of Increasing the Level of Security ensured by the Biometric Access Control System (Metoda zwiększania poziomu bezpieczeństwa zapewnianego przez system biometrycznej kontroli dostępu),* 'Electrotechnical Review' (Przegląd Elektrotechniczny) 2015, no. 10, p. 229.

access control system is the function of emergency door opening in the case of a fire. This function is performed after the transfer of information about the threat by the module (contact responsible for fire alarm).

An important element of the access control system is the development of procedures related to granting authorisations to the system users working in the facility subject to mandatory protection. It depends on the type of the facility and services provided at its premises. The access control system generally covers sensitive premises of the facility in which server rooms, switchgears, aggregates, ventilator rooms, heating substations, archives, means of direct coercion, administration, technical corridors, etc. are located. In the case of particularly important places (e.g. places where personal data are processed), two-step authentication process is recommended[25]. The intrusion and assault warning system identifies authorised persons and alarms the administrator on an ongoing basis about an unauthorised entry.

4.2. Intrusion and Assault Warning System

Another system of technical security measures applied in facilities subject to mandatory protection is the intrusion and assault warning system. Its purpose is to secure a given area or premises against intrusion of an unauthorised person (burglary, assault, theft) through detecting the intruder and sending an appropriate alarm to the operator. It can be divided into: the intrusion warning system and the assault warning system.

The purpose of the intrusion warning system is to secure premises against the intrusion of unauthorised persons. In the case of the facility operation during a day, the security with the use of detectors should be limited only to the areas without permanent presence of persons. During working hours signals from detectors should be blocked so that the presence of staff or clients natural in this period do not trigger an alarm. For this purpose, it is justified to divide the facility into zones resulting from functions performed by premises covered by them or from authorisations of persons who work in these premises. At night, the scope of operation of the intrusion warning system should be extended to the entire facility to allow detecting the intruder as soon as possible.

The task of the intrusion warning system is to transfer the information about a direct threat of intrusion. For reasons of safety of employees and clients, the information about the alarm should be delivered to security staff and other persons liable for taking actions. Elements of the intrusion warning system include manual panic buttons not triggering an alarm on the site. Most frequently the intrusion and assault warning system in facilities is designed to meet the second level of protection. Premises of local server rooms and external cabinets of the video surveillance system may be the exception. In this case, the third level of protection should be met. This system is applied mainly to secure technical premises, places of storage of valuable things, cash registers, transformer stations or CCTV network switches. For this purpose, opening, dual and PIR detectors are used. After detecting by the detector a violation of the surveillance zone or pressing the panic button, an appropriate signal is sent to the alarm centre of the intrusion and assault

[25] Judgement of the Provincial Administrative Court in Warsaw of 3 September 2020, II SA/Wa 2559/19. LEX no. 3077973.

warning system, which transmits a signal through a communications device to the system operator[26].

Good practice is to divide protected premises and devices into surveillance zones covered by the supervision performed by employees holding appropriate codes and authorisations. Each authorised person has an individual code allowing an appropriate access differentiated depending on authorisations concerning access to individual zones and functions. The intrusion and assault warning system in the facility subject to mandatory protection should be equipped with emergency power supply, which determines the proper operation irrespective of the main power supply.

The system recognises several types of alarms handled by the operator on an ongoing basis. It is justified that casings of detectors and panic buttons have a tampering alarm, and the monitoring lines are equipped with resistors protecting against destruction of the entire line or central unit in the case of short circuit.

4.3. Video Surveillance System

The use of CCTV cameras constitutes the most common tool for securing protected places. It fulfils the following extremely important roles[27]:

- an active role – supervision, counteracting threats;
- a passive role – evidence in the case, management of crisis situations;
- a training role – analysis of the threat and assessment of actions undertaken.

In facilities subject to mandatory protection, cameras with different resolution and functions are used. The choice of a specific type of camera at a given place should be preceded by the analysis of exposure of this place to threats, which then should be taken into account at the stage of designing the system. Fixed cameras have constant viewing areas, while speed dome cameras may have predefined patrol routes or rotate in accordance with the instructions of the monitoring operator.

On the market there are cameras with different possibilities. Their additional functions significantly support physical protection in ensuring security of the facility due to the possibility to patrol places (PTZ cameras) or to register sound. Cameras with the image analytics function are particularly useful. The camera records people's behaviours and on this basis transfers to the monitoring centre such alerts as: unattended luggage or violation of the designated security line.

The appropriate equipment of the workstation of CCTV monitoring operator is of extremely importance. The number of monitors receiving images from cameras should be adequate to the number of operators. The effectiveness of observations and thereby the effectiveness of monitoring become lower with the increase of monitors handled by one employee (table 1).

---

[26] M. Buczaj, A. Sumorek, *Virtual Surveillance System Controlling the Operation of the Intrusion and Assault Warning System (Wirtualny system nadzoru sterujący pracą systemu sygnalizacji włamania i napadu).* 'Motrol' 2010, no. 12, p. 49.

[27] C. Mecwaldowski, *Organisation of the Observer Place in the Video Surveillance System (Organizacja stanowiska obserwatora w systemie monitoringu wideo),* [in:] K. Jędrzejak. M. Tomaszewska-Michalak (ed.), *Technology in the Penitentiary Protection. Cooperation: Human Being-Technology (Technologia w ochronie penitencjarnej. Współpraca: cztowiek-technika),* Warsaw 2017, p. 84.

Table 1. Effectiveness of observations depending on the number of monitors

Number of monitors	1	4	6	9
Effectiveness of observations	85%	74%	58%	53%

Source: J. Wood, *CCTV – human factor challenges,* Nordic Ergonomics Society Annual Conference 2014

It is assumed that the maximum number of images observed by the operator should be from 12 to 16 monitors[28]. The practice of organising monitoring centres shows that employees often operate a significantly greater number of monitors, which results in the reduction of effectiveness in detecting events. A lot also depends on complexity of images observed by the monitoring operator, however in the literature on the subject there is no explanation of the concept of complexity[29]. The cause of the above problems is the trend to limit costs resulting from the employment of additional employees. Therefore, in order to ensure the optimal level of security, it is justified to determine the minimum number of monitoring operators in relation to the general number of images displayed on monitors with a view of maintaining the appropriate effectiveness of observations. The appropriate document for the inclusion of this type of recommendations is *the Methodology of agreeing protection plans of areas, facilities and devices subject to mandatory protection*, developed by the National Police Headquarters.

5. Conclusion

The introduction of the obligation to protect areas, facilities and devices important for state security with the use of internal security services or personal and property protection agencies constitutes new quality both in the legislative as well as institutional and organisational dimension. Guaranteeing the appropriate level of safety of all units subject to mandatory protection is not possible only with the use of state services performing a wide range of tasks. The necessity to use personal and property protection agencies and the individual approach to ensuring safety of a specific entity included in the register of the province governor constitute a kind of *signum temporis*.

Practical manner of ensuring safety of areas, facilities and devices important from the point of view of the state and its defence consists in the synchronous use of physical protection and technical security systems. The use of only one method of protection does not allow obtaining the optimal level of security although such a possibility is provided for in the Polish Act of 22 August 1997 on protection of persons and property. The adopted hypothesis – referring to the legal and organisational dimension of operations leading to ensuring safety of areas, facilities and devices subject to mandatory protection – has been verified positively.

Carrying out the analysis of methods of physical protection and technical security measures applied in facilities subject to mandatory protection has allowed distinguishing a number of functions performed by internal security services or personal and property protection agencies in order to ensure the appropriate

[28] *Ibidem,* p. 91.

[29] R. Pikaar, D. Lenior, *Human Factors Guidelines for CCTV control centre design. Introduction to a Symposium,* Nordic Ergonomics Society Annual Conference 2014.

level of safety. These include:

- control function – constant observation and supervision over the facility safety;
- preventive function – preventing violations of law, regulations of the facility, occurrence of crimes, offences or fights at the premises of the facility;
- reaction function – possibility to undertake immediate actions by the security staff adequate to the situation;
- coordination function – possibility to appropriately organise actions at the time of alarm from the system of technical security measures.

There is no doubt that new challenges in the scope of security of areas, facilities and devices subject to mandatory protection in the nearest future will be mainly connected with the need to adapt the technology used in technical security measures to crisis situations caused e.g. by the pandemic situation. The COVID-19 epidemic has shown that in the face of biological threats the need for further research on algorithms using artificial intelligence and machine learning is noticeable. It may constitute an inspiration for further development of remote monitoring systems, which will allow monitoring the body temperature of employees without the necessity of direct contact, which is extremely important in the context of the threat posed by the SARS-CoV-2 virus.

The necessity to include the State Fire Service in the process of agreeing protection plans of areas, facilities and devices subject to mandatory protection is also noticed. Aspects related to fire protection included in the document are not consulted with the relevant Provincial Police Commander or the director of the branch office of the Internal Security Agency. Therefore, in order to maintain the appropriate level of fire safety, these issues should be supervised by the provincial commander of the State Fire Service.

To sum up, contemporary challenges and threats occurring in the safety area require cooperation of services, guards and inspections with the private sector. The main purpose of these measures is to prevent potential threats, taking into account also their hybrid dimension. The achievement of the purpose defined in this way depends to a great extent on taking part of the liability for the protection of areas, facilities and devices of strategic importance for the state and proper performance of assigned tasks by internal security services or personal and property protection agencies.

Bibliography

Legal acts:

1. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 21 października 2011 r. w sprawie zasad uzbrojenia specjalistycznych uzbrojonych formacji ochronnych i warunków przechowywania oraz ewidencjonowania broni i amunicji (Dz. U. 2011 nr 245 poz. 1462).
2. Ustawa z dnia 22 sierpnia 1997 r. o ochronie osób i mienia (Dz. U. 1997 nr 114 poz. 740).
3. Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. 2010 nr 182 poz. 1228).
4. Ustawa z dnia 29 października 2010 r. o rezerwach strategicznych (Dz. U. z 2017 poz. 1846 oraz z 2020 poz. 374).

5. Ustawa z dnia 24 maja 2013 r. o środkach przymusu bezpośredniego i broni palnej (Dz. U. 2013 poz. 628).

Scientific books and articles:

1. Buczaj M, Sumorek A., *Wirtualny system nadzoru sterujący pracą systemu sygnalizacji włamania i napadu,* „Motrol" 2010, nr 12.
2. Ćwirko R., Ćwirko J., *Modułowy system kontroli dostępu dla dydaktyki,* „Pomiary. Automatyka. Kontrola" 2014, r. 60, nr 9.
3. Dąbrowski T., Bednarek M., Wiśnios M., *Metoda zwiększania poziomu bezpieczeństwa zapewnianego przez system biometrycznej kontroli dostępu,* „Przegląd Elektrotechniczny" 2015, nr 10.
4. Gozdór G., *Ustawa o ochronie osób i mienia. Komentarz,* Warszawa 2005.
5. Kośmider T. (red.), *Środki przymusu bezpośredniego. Zakres i sposoby użycia na przykładzie wybranych podmiotów bezpieczeństwa,* Warszawa 2020.
6. Kośmider T., *Determinants of the process of creating national security,* „Journal of Security and Sustainability Issues" 2021, nr 11.
7. Kręgulec R., Pajorski P., *Ustawa o ochronie osób i mienia. Komentarz,* Warszawa 2015.
8. Mecwaldowski C, *Organizacja stanowiska obserwatora w systemie monitoringu wideo* [w:] K. Jędrzejak, M. Tomaszewska-Michalak (red.), *Technologia w ochronie penitencjarnej. Współpraca: człowiek-technika,* Warszawa 2017.
9. Misiuk A., Kalaman M., *Kierunki zmian organizacyjno-technicznych w Służbie Więziennej,* Warszawa 2016.
10. Pikaar R., Lenior D., *Human Factors Guidelines for CCTV control center design. Introduction to a Symposium,* Nordic Ergonomics Society Annual Conference 2014.
11. Wood J., *CCTV - human factor challenges,* Nordic Ergonomics Society Annual Conference 2014.

Case law:

1. Postanowienie Krajowej Izby Odwoławczej z dnia 28 października 2014 r., KIO 2094/14, LEX nr 1567433.
2. Wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie z dnia 3 września 2020 r, II SA/Wa 2559/19, LEX nr 3077973.