UDC 351.865:355.58 **https://doi.org/10.33405/2786-8613/2024/2/4/323342**

V. Zhabinskyi

Ye. Yakovenko

DESCRIPTION OF THE INTERNATIONAL STANDARD PROCESS FOR DETERMINING THE PROJECTED THREAT TO CRITICAL INFRASTRUCTURE FACILITIES

The article analyses potential threats to important state facilities and ways for the enemy to capture a vital Centre at a facility guarded by military units for the protection of important state facilities of the National Guard of Ukraine.

The author outlines the approaches of developed countries to identifying threats that may occur at a protected facility. International standards, which include the guidelines of the International Atomic Energy Agency (IAEA), are considered. Identification of potential threats to a facility is a planned standard procedure that is successfully implemented in developed countries.

Keywords: *nuclear power plants, governing bodies, vital centre, important state facilities, terrorist activity, potential threats, International Atomic Energy Agency, terrorist, criminal, protester, units for the protection of important state facilities of the National Guard of Ukraine.*

Statement of the problem. An important component of the combat training system of the National Guard of Ukraine (NGU) is the training of headquarters. The peculiarity of such training is that to ensure combat readiness, it is important to train not only the staff of headquarters, but also the non-staff headquarters of consolidated formations created together with other ministries and agencies. In addition, the wide range of tasks assigned to the NGU forces the command to choose a wide range of training topics to ensure that the command and control bodies are prepared to act in difficult circumstances, taking into account current internal and external threats to national security.

One of the main forms of training for the NGU command and control bodies is the command and staff faculty. It involves not only joint training of commanders and staffs, but also participation in interagency exercises using the international standard for determining the projected threat to critical infrastructure.

The fact that no terrorist organisations have existed or operated on the territory of Ukraine to date cannot guarantee that such a situation will not arise in the future. It is quite likely that Ukraine's vital interests will conflict with the interests of influential internal or external political or economic forces. In this case, the government will not make any concessions and will take a tough stance in defence of national interests. Such a situation could become a catalyst for attempts to resolve the issue by force, i.e. to initiate or activate local extremist and separatist cells or to export terrorist forces from outside.

Thus, the possibility of terrorist activity on the territory of Ukraine is quite real and there are no reasonable grounds to refute this claim. It is also possible to conduct such activities with appropriate financial support, due to the presence of extremist and separatist centres or the potential for a conflict of interest among social groups that could create such centres. In addition, the export of terrorist forces from abroad is likely. Therefore, despite the lack of precedents of terrorism in the past, the issue of protecting the population and vital centres, including important state facilities, from possible terrorist and sabotage acts in the future is relevant for Ukraine at the present stage.

Nuclear power plants (NPPs) are a very attractive target for a terrorist attack or sabotage. This is due, firstly, to their high potential danger. The Chornobyl disaster showed that an accident at such a facility has enormous long-term environmental and economic consequences, causing large casualties among the population. Such an accident could destabilise the social and political situation not only in a particular region but also in the country as a whole and have serious international consequences. Secondly, nuclear power plants play a very important role in the country's energy system. Almost 60 % of electricity generated in Ukraine is produced by four nuclear power plants. Therefore, the loss of at least one power unit will have serious energy and economic consequences due to the need to divert significant resources to compensate for the electricity shortage by

© V. Zhabinskyi, Ye. Yakovenko, 2024

increasing the capacity of other nuclear and thermal generators. In addition, nuclear power plants themselves are highly expensive. For example, the completion and commissioning of two units at Khmelnytsky and Rivne NPPs, which already had different degrees of readiness, was estimated at about $1.5 billion.

It should also be noted that the fact that the NPP premises were seized and held by attackers who do not even have the intention or capability to destroy the reactor is in itself a very resonant event that will attract the attention of the whole world. This was the case with the seizure of the Zaporizhzhia NPP, the largest nuclear power plant in Europe (with 6 power units), by the russian aggressor on the night of 4 March 2022. The seizure of a nuclear power plant, especially during a full-scale invasion, creates great opportunities for blackmailing the state authorities by the aggressor.

By seizing nuclear power plants, the aggressor pursues a number of goals.

1. Creating a reliable cover for its troops, because no one (except themselves) in their right mind would fight near a nuclear power plant.
2. Blackmailing Europe and the world with the threat of accidents at such a large-scale facility with radiation hazards.
3. Control over Ukraine's energy system.
4. Access to nuclear fuel loaded into the reactors, which could potentially become raw material for nuclear weapons.
5. Possibility of various sabotage acts, which the enemy will blame on the Armed Forces of Ukraine, as well as creating panic and massive flight of the population.

This danger poses a threat not only to Ukraine but also to the whole of Europe. Therefore, governing authorities must be prepared to neutralise a terrorist group that intends to seize a vital centre at a protected facility.

Analysis of recent research and publications. The issue of potential threats to important state facilities (ISF) and ways for an adversary to seize a vital centre at a facility guarded by a military unit for the protection of high-security facilities of the National Guard of Ukraine is partially addressed in regulatory documents and scientific publications.

For example, Resolutions [6, 7] define the list of nuclear facilities, nuclear materials, radioactive waste, other state-owned radiation sources, important state facilities, facilities subject to protection by the National Guard, and important facilities subject to protection and defence by the National Guard of Ukraine in a special period.

The Regulation [8] describes the organisation and procedure for the National Guard of Ukraine to protect nuclear facilities, nuclear materials, radioactive waste, other state-owned radiation sources, important state facilities, critical infrastructure and special cargo.

The Law of Ukraine [4] defines the monitoring of the security level of critical infrastructure facilities.

Various aspects of countering terrorist and sabotage threats at critical infrastructure facilities are studied in the works of scientists S. Belai, O. Batiuk, O. Komisarov, S. Pavlov, O. Cherkashyn [9, 10].

To date, there has been no analysis of potential threats to important state facilities and the methods that the enemy can use to capture a vital centre at a facility guarded by a military unit for the protection of the military equipment of the National Guard of Ukraine.

The purpose of the article is to describe the international standard process for determining the projected threat to critical infrastructure protected by the military unit for the protection of the military assets of the National Guard of Ukraine.

To achieve this goal, the following partial tasks have been implemented:

– analysis of potential threats to important state facilities;
– describing the international standard process for determining the projected threat to critical infrastructure;
– identifying ways that an adversary could use to capture a vital centre at a protected facility.

Summary of the main material. The wide range of tasks assigned to the NGU [1] requires the command to conduct a wide range of exercises to ensure the readiness of the command and control bodies to act in difficult conditions, taking into account current internal and external threats to national security. The units for the protection of the NGU ISF [6, 7], which constitute an important element of the system of physical protection of especially important state facilities, are no exception.

The preparation of the NGU ISF protection units for emergency actions should be based on an assessment of potential threats identified by the state. In other words, the topics of different types of exercises should logically follow from the analysis of potential threats to critical infrastructure.

Let us consider the approaches of developed countries to identifying threats that may occur at a protected facility. The guidelines of the International Atomic Energy Agency (IAEA) contain standards according to which the identification of potential threats to a facility is a planned standard procedure that is successfully implemented by developed countries.

First of all, it is advisable to define the basic concepts.

Threat is the presence of a person or group of persons who have the potential (motivation, intentions, capabilities) to commit an undesirable action.

Threat assessment is the process of analysing and documenting the likely motives, intentions and capabilities of potential perpetrators that could cause undesirable consequences for nuclear materials and nuclear facilities.

Project threat assessment is a process conducted by competent authorities that comprehensively assesses factors to determine the project threat based on a threat assessment document.

Project threat is the properties and characteristics of potential internal or external perpetrators intending to unauthorisedly remove nuclear material, explosives or sabotage. A physical protection system is designed and evaluated to counter such intentions.

Persons interested in the assessment process (security system designers) make assumptions about the intentions of a potential intruder and their capabilities to cause damage to the protected facility. For example, terrorists, criminals, or protesters are attempting to take over a protected facility or commit sabotage, steal nuclear material, or commit other nuclear-related crimes.

Physical protection systems for critical facilities and transport of nuclear materials [3, 5] should be based on a threat assessment conducted by the state. The threat assessment determines the properties and characteristics of an offender who may attempt to steal nuclear materials or commit sabotage at a protected facility. Based on such an assessment, the competent state authority determines the design threat, which is taken into account when designing and assessing the physical protection system at the nuclear facility level.

The design threat is an essential element of the state physical protection system. Security experts assess the possible consequences of malicious acts in the area of the design basis threat. The project threat is also determined in relation to the transport of nuclear materials. Detection and detention of a moving vehicle requires different measures than in a stationary facility. The retaliatory forces accompanying the vehicle must neutralise the intruder before he attempts to steal nuclear material or commit sabotage.

The government allocates budgetary funds for physical protection of protected facilities. A decision is made to purchase certain types of equipment and to hire and train appropriate security personnel.

The international standard process for determining a project threat includes the following steps.

Step one: identifying the roles and responsibilities of all organisations.

Step two: developing predictions that are used in the threat assessment.

Step three: classifying external and internal threats into categories.

Step four: determining what you need to know about the threat (motives, intentions, capabilities).

Step five: identify sources of information about the threat.

Step six: collecting data on the threat.

Step seven: formalising the threat assessment and agreeing on positions on it.

Step eight: identifying the project threat based on the threat assessment.

Step nine: implementing the project threat into the regulatory framework.

Let's look at each step in sequence.

Step one: identify the roles and responsibilities of all organisations. The regulatory authority has the overall responsibility for identifying the project threat and implementing it. Success can only be achieved through the joint efforts of organisations that include intelligence agencies, state and local law enforcement, customs, and the Ministry of Defence. The state leadership empowers the regulatory authority to request support from various organisations to ensure that the project threat is credible and based on the latest intelligence. The authority to interact with other organisations provides a mechanism for obtaining the necessary secret and confidential information.

Step two: is to develop predictions that are used in threat assessments. There are many different threats in the world today. The threat assessment process, which will include consideration of all possible and existing threats that pose a risk to nuclear materials or facilities, will result in a number of working proposals or ground rules.

Step three: categorising external and internal threats. The IAEA recommends that states take into account both external and internal perpetrators. The external threat can be divided into three categories:

– terrorists (terrorist group);
– criminals;
– protesters.

The internal threat is usually divided into the following categories:
– passive;
– active violent;
– active non-violent.

Let's take a closer look at the individual categories.

An external intruder is an armed person who uses force, cunning, or deception to attack a facility. He may prepare his attack plan and carry it out with the help of internal intruders. External perpetrators may be terrorists or criminals intending to steal nuclear material or commit sabotage.

A terrorist is a person who threatens or commits violent acts to advance his or her demands. This can be a citizen of a country who disagrees with the government's policy and opposes it by various means. A terrorist motivated by an idea intends to commit sabotage against a facility or steal nuclear material. It is assumed that he will carry out an open attack on a nuclear facility and is prepared to die during the sabotage. He is a member of an armed, well-trained group with significant financial resources and a robust infrastructure. Terrorists may receive financial or logistical support from another state or terrorist organisation.

A terrorist group is a small group assisted by an insider (someone working at a nuclear facility) and may have a variety of equipment and explosives, machine guns, assault rifles, and even anti-tank grenade launchers. Terrorists are trained to conduct hostilities and sabotage. They may receive financial and personnel support from other states, as well as access to communications. They can use various types of vehicles (land, air and water), so an effective physical protection system is required.

A criminal is a person motivated by money who will not commit sabotage without material gain. The criminal intends to steal nuclear material or products of the military-industrial complex, and is convinced that it is very expensive. He may enter into a criminal conspiracy with an internal offender, and is not ready to die. The offender may be a member of an organised criminal group with significant financial resources.

A criminal group poses the following threat:
– it consists of two or more criminals;
– if there are more criminals, it may have links to organised crime;
– has conventional weapons;
– has a small amount of explosives;
– uses deception, kidnapping, coercion and extortion;
– its participants do not intend to die and may use violence;
– its participants do not understand the equipment.

A protester is a person who is motivated by the idea of a complete ban on the use of nuclear energy and seeks to put the facility at a disadvantage by demonstrating the ineffectiveness of the physical protection system. A group of protesters may include different subgroups: those with peaceful intentions and those who are ready to commit violent acts. Offenders may collude with an insider threat.

An insider threat is defined as a person who has unauthorised access to a facility without an escort. Insiders can be passive or active. A passive intruder is someone who provides information to other intruders. Alone or in collusion with external intruders, they will not pose a threat. Active perpetrators, in collusion with an external perpetrator or on their own, are capable of committing illegal acts accompanied by violence.

Collusion between an external and an internal intruder should also be considered in the assessment process, thus ensuring that the physical protection system can withstand an attack from an external intruder supported by an internal intruder.

Step four: determining what to know about the threat (motives, intentions, capabilities). After identifying the likely perpetrators, the regulator must determine what it needs to know about the perpetrators. Some violators may have the motivation and intent to commit a malicious act, but they do not have the capacity

to do so. Having fully identified the motives, intentions and capabilities of the potential intruder, the regulatory authority should also identify the threats to the protection of the facilities.

Step five: identify sources of information about the threat. After identifying the perpetrators to consider and the data for each threat, the regulator identifies the sources of information. Analysts can draw on a variety of reliable sources of information to assist in threat identification. Threat assessment organisations try to find all possible sources of information, but the information must be reliable and credible. The most reliable source of information comes from intelligence agencies. They have the ability to collect and analyse data to provide the latest and most reliable information needed to conduct a realistic threat assessment.

The nuclear industry is subject to few attacks, so analysts draw conclusions about threats based on events in related areas. For example, attacks on embassies, government buildings and personal property were analysed to identify relevant information. The analysts believe that the physical defence system is an effective means of preventing attacks, and therefore there have been minimal attacks on particularly important targets. Other sources of information include the following:

– Ministry of Foreign Affairs annual report on global terrorism;
– information services;
– list of events that took place at nuclear power plants;
– annual data of the Anti-Terrorism Centre on terrorist attacks.

The study of crimes committed in the vicinity of a facility, nationally and internationally, in the past and today, provides useful information. When there is a lack of data on incidents and crimes at protected facilities that would allow us to identify the characteristics of potential offenders, analysts expand their research to include crimes that are not directly related to the nuclear industry but are similar. A whole range of crimes is being analysed:

– robberies with the use of the latest technical means;
– high-profile armed robberies;
– industrial sabotage;
– crimes committed by professionals;
– cases involving political extremists, such as terrorist acts or "symbolic" attacks, the main purpose of which was to express political beliefs rather than destroy the target.

Step six: collecting and summarising threat data. At this stage, information needs to be collected, summarised and then analysed. The types of threats to nuclear facilities are different from those to other critical state assets. In the country, nuclear power plants may be threatened by the following: hijacking, unauthorised removal of special nuclear material, sabotage at a nuclear facility.

Step seven: formalise the threat assessment and agree on a position on the threat. Once the coordinating body has conducted the threat assessment and is confident that all possible threat data has been collected and analysed, it is important for the designated organisations to verify the complexity and likelihood of the threat to the state's nuclear industry. The working proposals are also reviewed to ensure their implementation in the threat assessment process. This step requires experts to discuss the credibility and realism of the projected threat and agree on positions in this regard.

Thus, the coordinating body has a realistic and reliable threat assessment [2, 4]. This document becomes the main one for determining the design basis threat and will be used by nuclear facilities in the design, implementation and evaluation of their physical protection systems.

Step eight: determining the project threat based on the threat assessment. The coordinating body makes a number of policy decisions on which threats critical facilities should be protected against [3, 4, 7, 8]. A wide range of issues is taken into account to determine which aspects of the threat assessment for the nuclear industry are most likely and which threats a nuclear facility should counteract.

Internal potential threats in the controlled area should be prevented by the security authorities of the protected facility [8]. The main task for the NGU is to counter external threats in the restricted area (see Table 1).

The coordinating body [4] should consider the following issues: the level of risk that the state is willing to accept at the national level; other national resources available to prevent a malicious act or mitigate its consequences; and the consequences that an attack on various facilities may lead to.

Table 1 – Summary data for determining the external project threat

External threats			
	Protesters	Criminals	Terrorists
Motives	Ideological idea	Material	Ideological
Intentions	Committing violent acts. Making demands	Kidnapping	Committing a terrorist act
Capabilities	Limited	Unlimited	Unlimited
Size of groups	Up to 1000 people	Criminal group (2–4 persons)	From 3 to 5 persons
Weapons	None	Small arms, explosives, bladed weapons	Pistols, bladed weapons
Explosives	None	Trinitrotoluene, TNT, TNT, ammonite, harmonite	Trinitrotoluene, TNT, TNT, ammonite, harmonite
Vehicles	Buses	Motorcycles	Buses, cars and trucks
Mechanical and hand tools	None	Lifts, various scissors, pry bars, lock picks, drills	Alpine equipment. Lifts, various scissors, pry bars, lock picks, drills
Training in the use of equipment	Low	High	High
Level of funding	One-time	Large financial resources	Large financial resources
Infrastructure	Unstable	Stable	Stable

The risk cannot be zero. The coordinating body should not exclude the possibility of a relevant attack threat, as well as the consequences of such an attack if it is successful. The Authority may determine that, for various reasons and factors, some threats of attack against a facility will not materialise, and therefore does not include them in the designated threat to the facility concerned. Thus, it exposes the facility to a certain risk. On the other hand, the coordinating authority may conclude that, although the threat of an attack is unlikely, the possible consequences of a successful attack would be very significant, and therefore the threat should be designated as a project-related threat.

The most difficult aspect of this process is determining the size of the attacker group that the facility must counter, as it has a direct impact on the physical protection system. Depending on the size of the attacker group defined in the design threat, the physical protection system may be overestimated or, conversely, insufficient. The probable size is determined by the regulatory authority on the basis of intelligence and information collected and analysed, as well as on the basis of a decision on the risk that may arise if the actual strength of the attackers far exceeds that determined by the design threat.

Step nine: introduction of the project threat into the regulatory framework of the state. This is the last step of the mentioned process. The legislative framework [2, 4] or the rules will oblige the nuclear facility to use the design threat in the process of designing protection and assessing the security of the facility. When the authority is determined, the regulatory body develops and establishes rules for the implementation of the design and evaluation process. The Ministry of Fuel and Energy begins this process by issuing guidance documents and orders that establish basic criteria and characteristics. A nuclear facility must meet these criteria and characteristics. The guiding documents and orders contain all the requirements for the physical protection system and are a guide for installations and objects for the implementation of a physical protection system that will effectively resist the violator envisaged in the project threat. Each facility develops guarantees and a safety plan at the facility, detailing the stages of compliance with the requirements of the governing documents and orders.

Each facility undergoes a comprehensive vulnerability assessment to determine the level of risk. The facility submits a report for approval to the relevant ministries and agencies. This process involves site visits by experts who conduct some limited tests to verify the functionality of the physical protection system.

The purpose of such verification is to ensure that the facility provides a correct and accurate assessment of the effectiveness of the physical protection system. In case of doubts about the reliability of the design and evaluation of this system at the facility, specialists of the relevant ministries and departments initiate changes to improve the reliability of the physical protection system, after which a schedule for their implementation is drawn up. The object receives permission for further work if the physical protection system at the object satisfies the ministry's experts, meets all the requirements of the governing documents and can counteract the project threat.

A physical defense system designed to counter terrorists is usually more resistant than a physical defense system against an offender who is not so well prepared and does not have technical means (for example, he is going to steal nuclear material to improve his financial situation). However, a physical security system designed to counter both trespassers and terrorists may prove ineffective against large numbers of protesters, including a small group of extremists intent on infiltrating the facility to demonstrate the ineffectiveness of the physical security system. In order to ensure proper countermeasures against external violators of all types, it is necessary to evaluate the effectiveness of countermeasures against a wide range of violators.

Let's consider the methods that a violator can use to capture a vital center at an object protected by a unit of the National Guard of Ukraine. As already mentioned, internal potential threats (in the controlled zone) must be prevented by the regime bodies of the protected object, while the NGU [1] is tasked with countering only external threats in the prohibited zone.

There are a large number of methods used by an intruder to penetrate a protected object. The following methods were most often used.

– employment directly at the facility or contracting organizations (in particular, in military units for NPP protection, ISF);

– study of the security system;

– use of deficiencies in the transit regime at checkpoints for the passage of employees and vehicles;

– bribery of employees of the protected object who are able to sell or transfer their pass to the object;

– an attempt to break through the main fence of the protected facility using boards, fire engines, etc.;

– penetration of the protected object through underground and aerial communications;

– carrying out "ramming" of checkpoints for the passage of road and railway transport with heavy equipment, "jumping" through checkpoints to allow employees to pass, forging documents and passes;

– an attempt to break into a protected object with the help of a motor vehicle carrying loose cargo (sand, crushed stone, sawdust, etc.);

– use of special equipment (firefighting, medical) for the infiltration of terrorists into the protected object, including railway transport;

– transportation of explosives to the protected object by attaching them to the bottom of the car, placing them in spare wheels, gas tanks, etc.;

– bringing weapons, explosives in office equipment and packaging to the facility paper for printing;

– seizure of cars of the administration, regime body, command of a military unit for the purpose of transporting explosives, as well as terrorists, to a guarded facility;

– simultaneous attempts to penetrate in 2–3 places (one of them – for distraction) to the protected object.

Criminal acts related to nuclear materials and installations are the theft of property that can be profitably sold. Stolen nuclear materials are very difficult to sell, so they are not always profitable for criminals.

A nuclear power plant is a complex technological facility. The equipment of life support systems and safety systems is duplicated, so several elements of these systems can be subjected to sabotage at the same time. The group of violators must have a large amount of explosives, special equipment, tools and will be numerous. Part of the attackers may be distracted by measures to maintain the captured premises and monitor their personnel. Therefore, in order to commit sabotage or a terrorist act at the facility, the attackers will need a large number of people, explosives, and tools. The more people participate in the attack, the easier it is for them to resist the security forces, the more explosives and special means will be delivered to the object, the more tasks can be performed simultaneously on the captured object, the easier it is to hold the captured premises. It can be argued that the probability of the attackers successfully carrying out the planned actions against the object directly depends on their number.

However, the value of the probability of success of covert or disguised actions is inversely dependent on the number of attackers, that is, the larger the group, the more likely it is to be detected during attempts to covertly or disguisedly enter the object and act there.

So, there is a contradiction: on the one hand, the large number of the group makes covert or masked penetration and further actions impossible, on the other hand, the small number (which makes covert

or masked penetration possible) does not make it possible to successfully complete the task. The use of assault tactics does not contain such confusion, which is its important advantage. In this case, the number of the enemy group is limited only by the possibility of organized arrival and assembly with weapons and special means in the area of the location of the object.

In the case of an attempt to covertly enter the territory of the object, bypassing the signaling border, there is a high probability of accidental interference, which will contribute to detection and disrupt the further execution of the task. Such an obstacle can be the unexpected appearance of a person from the staff of the station or guard, unscheduled inspection of posts, etc. The detection of attackers can also lead to careless crossing of the signaling line, and in this case, the attackers may not even notice that they have been detected, continue their actions and fall into a trap.

When attempting to cross checkpoints with forged documents in disguise, there is a chance of being detected by a document checker or a person who knows the face of the owner of the genuine documents. Even in the case of collusion with a person at the checkpoint, the disruption of the operation can be caused by the unexpected replacement of this person at the post, the arrival of persons with verification of service, etc. others

The use of assault tactics during an attack practically excludes the influence on the final result of the factors mentioned above, because the detection of the attack is foreseen by the process of preparing the operation and does not lead to disruption of the planned course of action. The sudden appearance of individuals, even armed ones, does not pose a serious threat considering the number and weapons of the attackers. Therefore, an attack using assault tactics is characterized by a low sensitivity of its result to unexpected changes in the situation, possible in the case under consideration. This is also a significant advantage of assault tactics for the violator.

In the case of covert penetration, among the factors that affect the value of the probability of detecting an attack, at each stage, subjective factors play a significant role (the appearance of a station worker, the choice of a specific time and route of the inspection by the person checking the guard service, etc.), for which it is practically impossible determine the distribution law and other probabilistic parameters, but which cannot be ignored. Therefore, planned actions have a high level of non-stochastic uncertainty.

Situations when assault tactics are used are more predictable, as they will depend mostly on objective factors based on physical values (distance from the security boundary to the power unit housing, speed of movement of the attackers and alarm group of guards, time to overcome the barrier strip, etc.). Some of these quantities are deterministic (for example, terrain distances), others (time to overcome a barrage, speed of advancement, etc.) are random. However, for the latter, it is still possible to determine probabilistic parameters, for example, by conducting training on full-scale models or by modeling.

In determining the course of an operation using assault tactics of attackers, objective factors are the main ones, so reliable forecasting of such an operation is quite possible.

Conclusions

Parts for the protection of the National Guard of Ukraine important state facilities are an important element of the system of physical protection of particularly important state facilities. A necessary condition for the sufficiency of the system of physical protection of particularly important state facilities is the training of the management bodies and personnel of the units in the protection of the National Guard of Ukraine important state facilities.

The preparation of units for the protection of important state facilities for actions under extraordinary circumstances should be based on the assessment of potential threats determined by the state and international standards.

The preparation of units for the protection of important state facilities for actions under extraordinary circumstances should be based on the assessment of potential threats determined by the state and international standards.

The basis for determining the adequacy of the physical protection system is the design threat. It sets the initial international standard for further changes in the system of physical protection of facilities to ensure a standardized level of protection for all facilities. As new information becomes available, the design threat must be constantly evaluated to ensure its validity and reliability, as it is the basis for designing and evaluating the physical protection system. Acquisition of new opportunities by violators requires constant changes from the project threat in accordance with the change in threats.

The facility's physical protection system must take into account both external and internal threats. As a rule, the external threat consists of three categories: terrorists, criminals, protesters.

The internal threat can also be of three categories: passive, active non-violent, active violent.

Prevention of internal potential threats in the controlled area is entrusted to the regime bodies of the protected object. The task of the National Guard of Ukraine is to counter external threats in the restricted area of the protected facility.

A system of physical protection, which provides for countering terrorists, is usually more stable than a system of physical protection, which counters a violator, who is not so well prepared and without technical means. A terrorist motivated by an idea intends to sabotage a facility or steal nuclear material. He is a member of an armed and well-trained group with large financial resources and a stable infrastructure. It is assumed that terrorists will carry out an open attack on a nuclear facility and are ready to die during the act of sabotage.

Therefore, the management bodies of the protection unit of the National Guard of Ukraine important state facilities must be ready to participate in actions to neutralize a terrorist group that is trying to capture a protected critical infrastructure object.

The prospect of further scientific work will be the study of the peculiarities of the interaction of the security forces, the management bodies of the parts for the protection of the important state facilities of National Guard of Ukraine, the relevant ministries and agencies regarding the improvement of the system of protection and defense of critical infrastructure objects.

References

1. *Zakon Ukrainy "Pro Natsionalnu hvardiiu Ukrainy" № 876-VII* [Law of Ukraine about the Natsional Guard Ukraine activity no. 876-VII]. (2014, March 13). Retrieved from: http://surl.li/qeqja (accessed 10 September 2024) [in Ukrainian].

2. *Zakon Ukrainy "Pro natsionalnu bezpeku Ukrainy" № 2469-VIII* [Law of Ukraine about the National Security of Ukraine activity no. 2469-VIII]. (2018, June 21). Retrieved from: https://zakon.rada.gov.ua/laws/show/2469-19#Text (accessed 10 September 2024) [in Ukrainian].

3. *Zakon Ukrainy "Pro fizychnyi zakhyst yadernykh ustanovok, yadernykh materialiv, radioaktyvnykh vidkhodiv, inshykh dzherel ionizuiuchoho vyprominiuvannia" № 2064-III* [Law of Ukraine about the physical protection of nuclear installations, nuclear materials, radioactive waste, and other sources of ionizing radiation activity no. 2064-III]. (2022, October 16). Retrieved from: http://surl.li/kutuqp (accessed 10 September 2024) [in Ukrainian].

4. *Zakon Ukrainy "Pro krytychnu infrastrukturu" № 1882-IX* [Law of Ukraine about the Critical Infrastructure activity no. 1882-IX]. (2024, September 21). Retrieved from: https://zakon.rada.gov.ua/laws/show/1882-20#Text (accessed 10 September 2024) [in Ukrainian].

5. *Postanova Kabinetu Ministriv Ukrainy "Pro zatverdzhennia pereliku spetsialnykh vantazhiv, yaki pidliahaiut okhoroni ta oboroni Natsionalnoiu hvardiieiu Ukrainy" № 338* [Resolution of the Cabinet of Ministers of Ukraine "On approval of the list of special cargoes subject to protection and defense by the National Guard of Ukraine" activity no. 338]. (2014, August 13). Retrieved from: http://surl.li/nsqxlk (accessed 10 September 2024) [in Ukrainian].

6. *Postanova Kabinetu Ministriv Ukrainy "Pro zatverdzhennia pereliku yadernykh ustanovok, yadernykh materialiv, radioaktyvnykh vidkhodiv, inshykh dzherel ionizuiuchoho vyprominiuvannia derzhavnoi vlasnosti, vazhlyvykh derzhavnykh obiektiv, obiektiv, shcho pidliahaiut okhoroni Natsionalnoiu hvardiieiu" № 628* [Resolution of the Cabinet of Ministers of Ukraine "On approval of the list of state-owned nuclear facilities, nuclear materials, radioactive waste, other sources of ionizing radiation, important state facilities, and facilities subject to protection by the National Guard" activity no. 628]. (2014, November 12). Retrieved from: http://surl.li/obafdc (accessed 10 September 2024) [in Ukrainian].

7. *Postanova Kabinetu Ministriv Ukrainy "Pro zatverdzhennia perelikiv vazhlyvykh obiektiv, yaki pidliahaiut okhoroni ta oboroni Natsionalnoiu hvardiieiu Ukrainy v osoblyvyi period" № 685-011* [Resolution of the Cabinet of Ministers of Ukraine "On approval of lists of important objects subject to protection and defense by the National Guard of Ukraine in a special period" activity no. 685-011]. (2021, July 7) [in Ukrainian].

8. *Nakaz Ministerstva vnutrishnikh sprav Ukrainy "Pro zatverdzhennia Polozhennia pro orhanizatsiiu i poriadok nesennia sluzhby z okhorony yadernykh ustanovok, yadernykh materialiv, radioaktyvnykh vidkhodiv, inshykh dzherel ionizuiuchoho vyprominiuvannia derzhavnoi vlasnosti, vazhlyvykh derzhavnykh obiektiv, obiektiv krytychnoi infrastruktury ta spetsialnykh vantazhiv Natsionalnoiu hvardiieiu Ukrainy" № 497* [Order of the Ministry of Internal Affairs of Ukraine "On the approval of the Regulation on the organization and procedure for the protection of nuclear installations, nuclear materials, radioactive waste, other sources

of state-owned ionizing radiation, important state facilities, critical infrastructure facilities and special cargo by the National Guard of Ukraine" activity no. 497]. (2023, June 15). Retrieved from: https://docs.dtkt.ua/doc/z1085-23 (accessed 10 September 2024) [in Ukrainian].

9. Komisarov O. H., Bielai S. V., Cherkashyn O. D. (2020). *Obgruntuvannia zavdan ta povnovazhen Natsionalnoi hvardii Ukrainy shchodo zakhystu obiektiv krytychnoi infrastruktury* [Justification of the tasks and powers of the National Guard of Ukraine regarding the protection of critical infrastructure facilities]. *Chest i zakon*, no. 2. (73), pp. 99–106 [in Ukrainian].

10. Komisarov O. H., Batiuk O. V., Pavlov S. P. (2021). *Kryminalistychne ta sluzhbovo-boiove zabezpechennia protydii terorystychnii ta dyversiinii zahrozam na obiektakh krytychnoi infrastruktury* [Forensic and service-combat support against terrorist and sabotage threats at critical infrastructure facilities]. *Chest i zakon*, no. 4. (79), pp. 33–39 [in Ukrainian].

The article was submitted to the editorial office on 6.12.2024

УДК 351.865:355.58

В. М. Жабінський, Є. С. Яковенко

ОПИС МІЖНАРОДНОГО СТАНДАРТНОГО ПРОЦЕСУ ВИЗНАЧЕННЯ ПРОЄКТНОЇ ЗАГРОЗИ ОБ'ЄКТАМ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Проаналізовано потенційні загрози важливим державним об'єктам і способи захоплення противником життєво важливого центру на об'єкті, що охороняється військовими частинами з охорони важливих державних об'єктів Національної гвардії України.

Окреслено підходи розвинених країн світу до визначення загроз, які можуть мати місце на об'єкті, що охороняється. Розглянуто міжнародні стандарти, котрі містять керівні документи Міжнародного агентства з атомної енергетики (МАГАТЕ). Визначення потенційних загроз об'єкту являє собою планову стандартну процедуру, що успішно реалізується в розвинених країнах світу.

Частини з охорони важливих державних об'єктів Національної гвардії України – важливий елемент системи фізичного захисту особливо важливих об'єктів держави. Необхідною умовою достатності системи фізичного захисту особливо важливих об'єктів держави є навченість органів управління і особового складу частин з охорони важливих державних об'єктів Національної гвардії України. Підготовка частин з охорони важливих державних об'єктів до дій за надзвичайних обставин має ґрунтуватися на оцінюванні потенційних загроз, визначених державою та міжнародними стандартами.

Основою для визначення достатності системи фізичного захисту є проєктна загроза, яка встановлює початковий міжнародний стандарт щодо подальших змін у системі фізичного захисту об'єктів для забезпечення стандартизованого рівня захисту для всіх об'єктів. У міру отримання новітньої інформації проєктну загрозу слід постійно оцінювати, аби забезпечити її достовірність і надійність, оскільки вона є базовою для проєктування й оцінювання системи фізичного захисту. Набуття порушниками нових можливостей потребує від проєктної загрози постійних змін відповідно до зміни загроз.

Система фізичного захисту об'єкта має враховувати як зовнішні, так і внутрішні загрози. Зовнішню загрозу, як правило, становлять три категорії: терористи, злочинці, протестувальники.

Внутрішня загроза також може бути трьох категорій: пасивна, активна ненасильницька, активна насильницька.

Ключові слова: *атомні електричні станції, органи управління, життєво важливий центр, важливі державні об'єкти, терористична діяльність, потенційні загрози, Міжнародне агентство з атомної енергетики, терорист, злочинець, протестувальник, частини з охорони важливих державних об'єктів Національної гвардії України.*

ZHABINSKYI Volodymyr – Senior Lecturer of the Department of State Security and Management of the National Academy of the National Guard of Ukraine
https://orcid.org/0000-0002-5085-6849

YAKOVENKO Yevhen – Candidate of Pedagogical Sciences, Deputy Head of the Command and Staff Faculty – Head of the Training Department of the National Academy of the National Guard of Ukraine
https://orcid.org/0000-0002-2612-8550