Prevention of Terrorist Effects on critical infrastructure objects using motor vehicle databases obtained from External Surveillance Video Systems

Mykhailo Diviziniuk[1] [0000-0002-5657-2302], Oleksandr Farrakhov[1] [0000-0003-4988-126X], Liubov Shaidetska [2][0000-0002-6593-0255], Maksym Dement [3][0000-0003-4975-384X], Olha Ryzhchenko [3][0000-0003-1693-6121]

[1] Center for Information-analytical and Technical Support of Nuclear Power Facilities Monitoring of the National Academy of Sciences of Ukraine, Kyiv, Ukraine
[2] National Technical University of Ukraine "Kyiv Polytechnic Institute named after Igor Sikorsky", Kyiv, Ukraine
[3] National University of Civil Defence of Ukraine, Kharkiv, Ukraine

farrakhov@ukr.net

Summary. The article shows new information and technical method development to prevent emergency situations of a terrorist nature using databases of motor vehicles obtained from external surveillance video systems. Emergency situations of a terrorist nature over the past decades and the possibility of their occurrence at critical infra to prevent emergency situations of a terrorist nature at protected objects were considered. New information and technical methods of preventing emergency situations of a terrorist nature have been developed using motor vehicle databases obtained from external surveillance video systems.

Key words: motor vehicles, video surveillance, critical infrastructure object, controlled zone, violator, physical protection.

1 Introduction

Prevention of emergencies of a terrorist nature is an urgent problem of our time. This issue caused discussions in Ukraine's scientific and administrative circles a few years ago. Now, there is no doubt that nothing is impossible for terror.

The use of motor vehicles for terrorist purposes is easy to understand. It is not easy to purchase firearms. In the USA there are tens of millions of firearms in civilian circulation. Even there, the terrorist could not obtain anything more terrible than an air pistol. But a low-tonnage truck is easy to rent. Note that the criminal who crushed people in Nice [1] also rented a truck a few days before the terrorist attack.

Of course, cars cannot be controlled as closely as weapons, explosives, or their precursors. However, tracking systems become widespread in transport. It will theoretically make difficult or even completely close access to intruders [2-8].

2 Description of hypothetical critical infrastructure object

A state's critical infrastructure comprises enterprises, networks, and systems. Their failure or malfunction can cause loss of control or significant damage at the national or regional level [9-17]. It includes the following: nuclear, thermal, and hydroelectric plants, metallurgical, chemical, and petrochemical plants, aircraft, machine, and shipbuilding plants; other state and private enterprises of strategic purpose. They are protected objects of critical infrastructure (OCI) [18-24] (Fig. 1). Special sanitary and controlled zones are established around them by the decision of the local and regional authorities in the interests of ensuring the reliable functioning and protection of these protected objects. Protection of these objects from terrorist action is an urgent problem. Its solution determines the survival of the civilian population and Ukraine as an independent state [25].

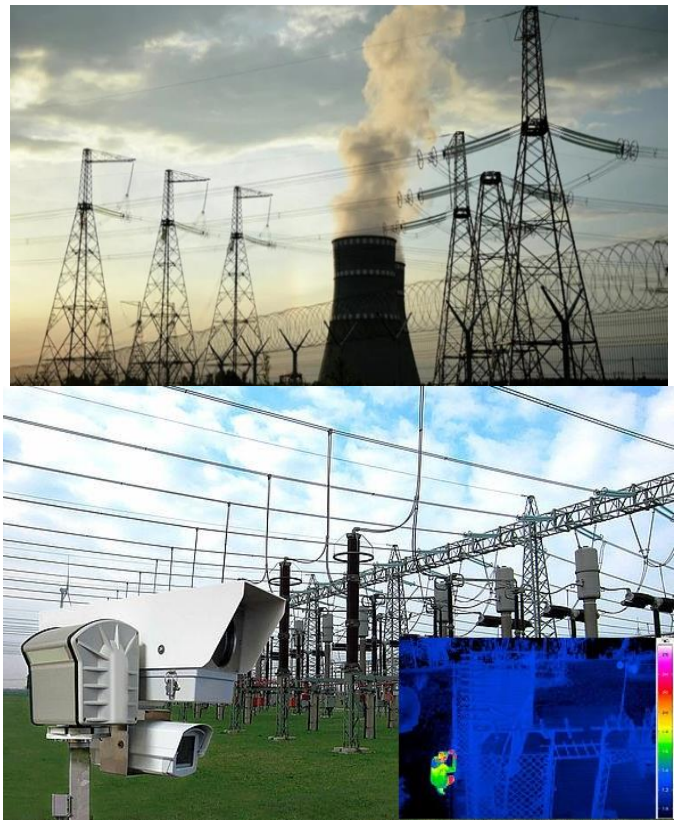

Fig. 1. Typical objects of critical infrastructure

Let’s consider a hypothetical object of critical infrastructure (Fig. 2).

The object itself is located in the center. The guarded perimeter consists of the main perimeter (MP) and the territory of high-voltage transformers where two high-voltage power lines depart. They are marked as PTL-1 and PTL-2 on the diagram.

There is an administrative building, nuclear reactors, and related turbine shops on the main territory of the protected facility. Their regular electricity was supplied. There are also rooms with emergency diesel generator sets, auxiliary rooms, garages, loading and unloading platforms, storage facilities for spent nuclear fuel and radioactive waste, and a cooling pond that provides the main production cycle. It is located in the lock connected with the river that flows nearby.

The protected perimeter of the OCI is equipped with six video systems with sufficient video cameras (shown by red dots on the diagram) to monitor the perimeter and the adjacent sanitary zone.

There are three more sites next to the object that are directly subordinated to the object: the car park, marked on the diagram as CP, and warehouses located on the sites marked on the diagram as Warehouses 1 and Warehouses 2. Four video systems (shown by blue dots on the diagram) are installed on these sites. They have sufficient video cameras to monitor the perimeter of the sites adjacent to this territory, entrance and exit from them. In total, video surveillance of the hypothetical OCI contains 21 video systems. Six provide the main territory and fifteen are auxiliary.

The facility is equipped with two railway checkpoints (checkpoints). They control railway access roads. Three road checkpoints prevent car access roads, and two pass through the car park.

Five villages are located around the protected object. There are farms in the first village. Two security video systems (blue stars) are installed within its borders. It protects farms and controls access roads. In the second village, there are greenhouses. Two security video systems (blue stars) are also installed there. It protects farms and controls access roads. The third village is a country where three video systems are installed (blue stars). The fourth village is characterized by the local population who work at the enterprises listed above. It is not equipped with video systems. Two video systems serve the railway station and approach roads (red stars). Nine video systems were installed in five villages, and a railway station was located next to the protected object. It provides their protection and control of access roads to them.

The CIF satellite city was built in close proximity to it. The facility staff and their families live here. A railway station is also equipped with two video systems (red stars on the diagram).

The railway line in this area is equipped with three more video systems (red stars on the diagram) in addition to the above-mentioned stations. They are installed on the branch roads and on the railway bridge on two sides.

The city is located on the bank of the river. The river shipping has two video systems installed on the river pier and two on the road bridge across the river (red stars on the diagram). It provides control over the river water area and record of the cars' flow crossing the river., The river shipping company installed a panoramic video system on the hill near Warehouse 1 (red stars on the diagram) in addition to monitoring the water area on the approaches to its berth.

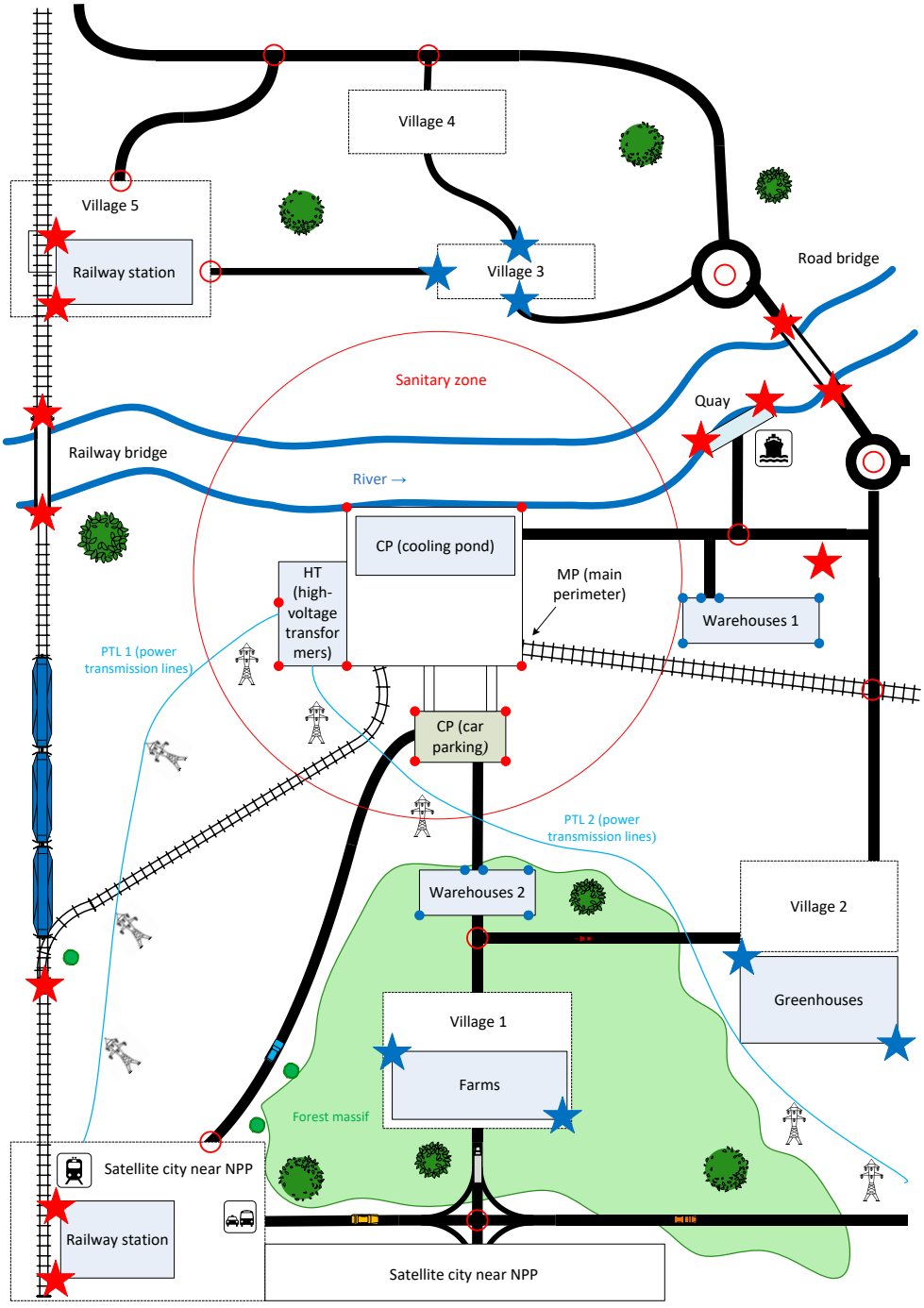

Fig. 2. Diagram of a hypothetical protected critical infrastructure object

Three more video systems are installed at all checkpoints of the protected object. One of them is located on the branch of the railway tracks connecting the railway with the object. The other two are located on the track before entering the satellite city, on the edge of the forest massif (green circles on the diagram).

CIF and its adjacent villages and the industrial site are connected by roads controlled by the patrol police of the Ministry of Internal Affairs of Ukraine. Video systems are installed to ensure automobile traffic safety on the roads. It provides control over the movement of vehicles in accident-hazardous places: at key intersections before entering the satellite city, at the intersection in front of the automobile bridge on both sides, at the intersections in front of going to the fourth and fifth villages, and to the satellite city (shown in the diagram with red circles).

Thus, the considered hypothetical guarded critical infrastructure object is equipped with 54 video surveillance systems that monitor the movement of all motor vehicles in a thirty-kilometer zone around the object. There are a total of 54 video systems. Twenty-four belong to the protected object, private structures, and other agencies install 19 systems, and 11 specialized video systems are intended for traffic safety control by the Ministry of Internal Affairs.

3 Scheme of collecting and filling a database

There is a huge flow of motor vehicles (motor vehicles) for various purposes near any critical infrastructure object.

Some move directly to the object, providing it with the necessary resources. Other vehicles ensure the functioning of enterprises and institutions located in the immediate vicinity of the protected object. The third ones transit through the controlled zone of the protected facility, the fourth ones provide intra-city needs, long-distance flights, and others.

Any vehicle belonging to one of the above groups can act as a potential violator (intruder) from the point of view of the anti-terrorist security of a critical infrastructure object. Therefore, we will classify motor vehicles.

It is possible to single out the first group of identification features, which consists of ten subgroups: 1) belonging to the protected object (object, near object, transit) and the owner of the vehicle; 2) destination (cargo, passenger, special); 3) appearance (brand, color, damage and other individual characteristics); 4) state, departmental or international registration number; 5) characteristics of the driver of the vehicle; 6) engine type and location; 7) structural features of the motor vehicle; 8) availability of a trailer, tug, and other auxiliary devices; 9) presence and characteristics of passengers; 10) availability and characteristics of the cargo.

The first group of identification signs can be conventionally called a group of static indicators (they remain constant during the vehicle operation). They allow you to fully identify the motor vehicle.

The identification features of the second group are dynamic characteristics that describe vehicle movement entering the control zone around the protected object. They include subgroups of markers that determine the car’s route: 1) departure point;

2) destination; 3) departure time; 4) time of arrival; 5) time and place of stops; 6) the purpose of these stops and their duration.

The database and knowledge base (Fig. 3) of motor vehicles operating near critical infrastructure facilities are formed based on groups of identification features. They include static and dynamic parameters that allow you to determine the vehicle and the nature of its movement unambiguously.

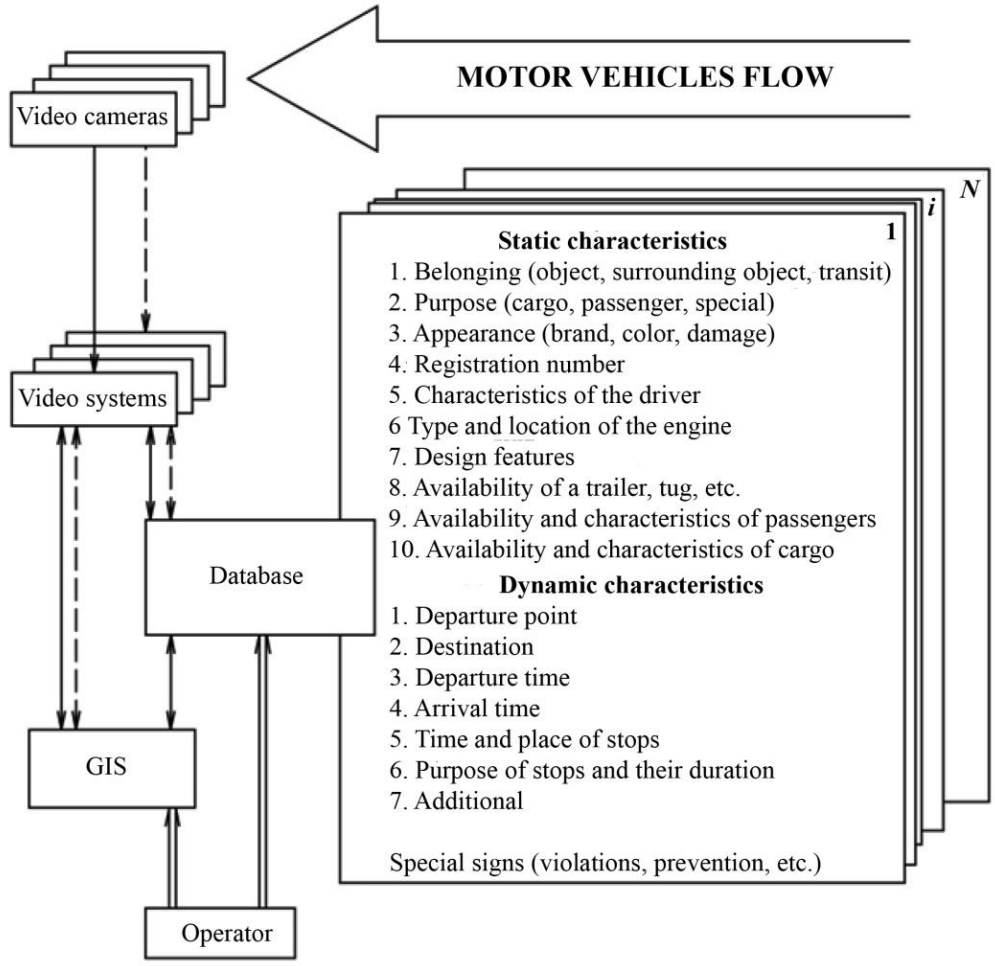

Fig. 3. Scheme of collecting and filling the database

Each vehicle's video recording clarifies, systematizes, and updates these characteristics.

An individual form of a motor vehicle includes special marks in addition to static and dynamic characteristics. These include all violations recorded by the system (deviations from the standard mode of vehicle use), the type of preventive effect on the driver, its results, and other data.

4 Mathematical model of detection of non-typical situations of terrorist nature

All vehicles passing by the protected object and located in its immediate vicinity are divided according to their belonging to the protected object into object, near-object, and transit.

There is a functional dependence w of the type (1) that connects the average statistical intensity σ traffic of motor vehicles (MV), which depends on the current fragment of the transport background Φ_i, traffic intensity $I\left(N,t\right)$ registered for a fixed period of time with the number of violators of the 1st and second H_2 levels. At the same time, the attacker may or may not be among them. This dependence determines the regular state of the situational background of motor vehicles moving near the critical infrastructure object.

$$W\left[\sigma\left(\Phi,t\right),I\left(N,t\right),H_1,H_2\right]=Const \quad (1)$$

Constant values are also determined by the limit value of the traffic intensity of vehicles registered by the video system at which reliable detection of violators is ensured.

The software used in the database and knowledge base allows for detection deviations from the standard characteristics of its use on five levels: violations of the 1st level are single deviations from the standard indicators of the MV use; violations of the 2nd level - are systematic or repeated deviations; violation of the 3rd level - are provocative actions; violations of the 4th and 5th level - are dangerous and clearly hostile actions.

Violations of the 3rd, 4th, and 5th levels are reported to the main control panel of the object's physical protection. The instructions describe these situations, and an adequate response is taken according to them.

Deviations from standard indicators of the use of 1st and 2nd levels of MV are collected in a particular risk group in the database and analyzed by specially trained personnel. The conclusion is made about the presence of signs characterizing the preparation of a terrorist act or other hostile actions against the guarded OCI based on the conducted analysis.

The number of violators is determined by specific fragments of the traffic background in the area controlled by video systems and by the amount of traffic intensity thresholds determining the mode of operation of video systems.

The total number of registered violators in the controlled zone of the protected object is determined by formula (2), taking into account the time factor that determines the relevant fragments of the traffic background

$$H=\sum_{j=1}^{l}\sum_{i=1}^{k}f_l\left(\Phi_i,\Pi,t\right) \quad (2)$$

where k – number of car traffic background fragments in the controlled zone around the protected object;

l – number of working video systems.

In other words, the number of abnormal situations detected by MV operating near OCI (violators) depends on the number of fragments of the traffic background and the number of working video systems in the controlled area and their modes of operation.

The process of registration and identification of MV, determination of violators of the 1st and 2nd level, and identifying potential intruders among them on a fixed fragment of the traffic background is a stationary Poisson flow. Now, the transition probabilities in the system do not depend on time. They are found by solving the system of differential equations (3) with constant coefficients:

$$\frac{dP_j(t)}{dt} = \sum_{i=1}^{N} H_{ij} P_i, \quad j = 1, 2, \ldots, N. \tag{3}$$

Moreover, several deviations from the standard characteristics of the use of the vehicle determine its transition from the group H_0 (supersets of registered vehicles) into H_1 (set of offenders of the first level) from H_1 to H_2 (set of offenders of the second level) from H_2 into H_3 (multiple potential intruders) regardless of the time interval during which these deviations were recorded.

Similarly, several measures regarding operational research, operational-preventive, and other actions are carried out by the competent authorities together with the physical protection service of the object, regardless of the period during which they are carried out. They determine the system's transition from the state H_3 into H_2, from H_2 into H_1, from H_1 into H_0, i.e. return to normal state.

By combining dependencies (1), (2), and (3), we will obtain a system that is an unknown mathematical model to detect non-typical situations of a terrorist nature using motor vehicles operating near a critical infrastructure facility:

$$\begin{cases} W\left[\sigma(\Phi, t), I(N, t), H_1, H_2\right] = C(\Pi), \\ H = \sum_{j=1}^{l} \sum_{i=1}^{k} f_l(\Phi_i, \Pi, t), \\ \frac{dP_j(t)}{dt} = \sum_{i=1}^{N} H_{ij}(t) P_i(t), \quad j = 1, 2, \ldots, N. \end{cases} \tag{4}$$

The mathematical model for detecting non-typical terrorist situations using motor vehicles operating near critical infrastructure facilities consists of three dependencies. The first describes the standard state of the situational background of motor vehicles operating near the object of critical infrastructure. It determines the limit value of the intensity of movement of vehicles registered by the video system when reliable detection of violators is ensured. The second equality allows you to choose the

number of violators or abnormal situations detected with motor vehicles operating near the protected critical infrastructure object, depending on the number of detailing fragments of the traffic background, the number of working video systems in the controlled area, and their modes of operation. The third dependence shows that the transition from the superset of registered vehicles to the set of violators of the 1st level, from it to the subset of violators of the 2nd level, and then to the set of potential intruders is determined by the number of deviations from the standard characteristics of the use of the vehicle, regardless of the recorded time interval. Similarly, the system's return to the normal state is determined by the number of measures carried out by the competent authorities and the protected object's physical protection service, regardless of the time interval during which they are carried out.

5 Scheme of the control algorithm of the information technology method

The control algorithm of the information-technical method of preventing terrorist emergencies using databases of motor vehicles obtained from external surveillance video systems is synthesized considering all the described schemes. Its scheme is shown in Fig. 4.

In general, the control algorithm consists of eight levels.

At the first level, there is a unit for determining gradations. The flow of incoming information is discretized while the operator manually enters the operating modes.

At the second level, the initial vehicle registration and data update unit automatically receives information on detecting new vehicle characteristics. It is delivered from lower levels via feedback lines. This is also the detailed information on the situational traffic background developing near the protected object.

The operator sets the sequence of updating data on motor vehicles in the database and knowledge by manual input.

At the third level, there is a unit for collecting, processing, and systematizing data on the situational background of motor vehicles. It compares data from external surveillance video systems on the static and dynamic characteristics of vehicles falling within the range of video cameras.

Systematic comparison of the registered (new ones coming from the video systems) characteristics with the parameters stored in the database and knowledge allows for detecting violations (deviations from the standard mode of use of vehicles). They are sent to the fourth level in the unit for detecting and systematizing violations.

Here, daily groups of violations are formed. It includes sets of monthly violations of the 1st level and subsets of violations of the 2nd level. Detected and systematized data on violations are sent to the two blocks located on the fifth level: the block for detecting new characteristics of vehicles and the block for detecting and systematizing violators. First, the registered violations (deviations from the regular mode of use of vehicles) are interpreted as new, previously unknown vehicle characteristics. They are automatically translated to the third level to the unit of collection, processing, and systematization of data on the situational background of motor vehicles and to the

second level to the unit of initial registration of vehicles and updating of data. Systematization and preparation for the separation of violators is carried out in the second.

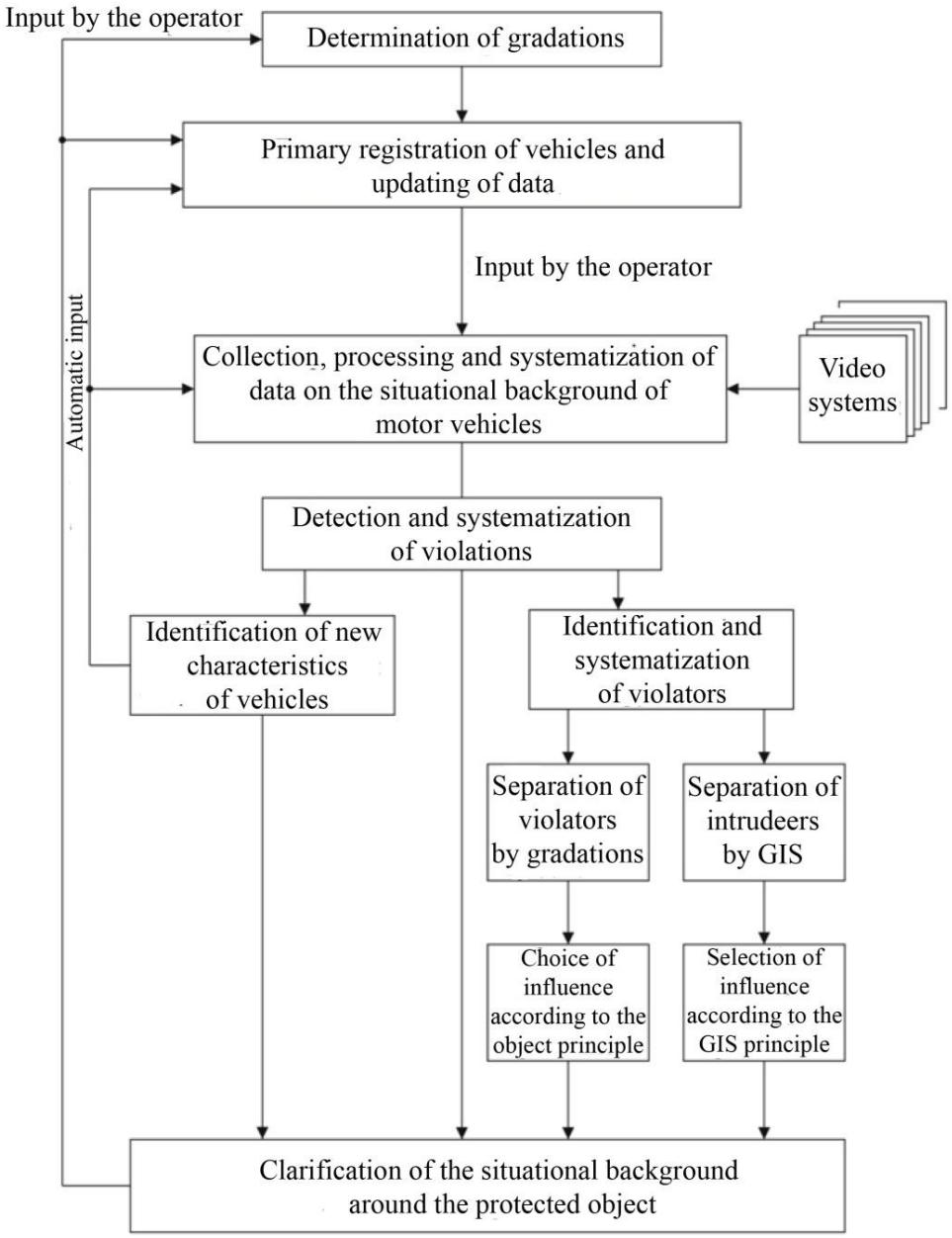

Fig. 4. Scheme of the control algorithm

There are two blocks on the sixth level. One divides violators according to gradations or by the criterion of belonging to a protected object. The second is divided by reference to the area or by geo-informational criterion. In both blocks, intruders are automatically classified by rating according to two characteristics: according to criterion H - the number of violations during the analyzed period, and according to criterion I - the intensity of violations during the analyzed period.

The received data is sorted by rating in the order of decreasing violations. It is translated into the corresponding blocks of the seventh level: selection block of influence according to the object principle and selection block of influence according to the geo-information principle. The developed types of influence are introduced manually by the operator.

Information from these blocks, together with the data from the block for detecting and systematizing violations (fourth level) and the block for detecting new vehicle characteristics (fifth level), is sent to the eighth level (the block for clarifying the situational background near the protected object). Then, the output data is sent to the second level from this block.

Thus, the control algorithm of the information and technical method of preventing terrorist emergencies using databases of motor vehicles obtained from external video surveillance systems is a hierarchical eight-level structure consisting of eleven sequentially connected blocks with four feedbacks. Its implementation ensures the processing of information constantly received from external surveillance video systems installed in the controlled area around the protected object. It detects violators (potential intruders) by double rating selection and preparation of the impact on them according to the object and geo-informational principles.

6 Description of the information and technical method of preventing emergencies of a terrorist nature

Use of the given method involves the following procedures: 1) determination of gradations and initial registration of vehicles; 2) systematization of data and knowledge about the situational background of motor vehicles in the controlled area around the protected object; 3) registration of violations and violators; 4) identification of potential intruders; 5) choice of impact on potential attackers.

The first procedure is a determination of gradations and initial registration of vehicles. It ensures the formalization of the entire hardware and software operation by defining appropriate time intervals. This is the definition of daily gradations into which investigated time intervals are divided (the period from 0 to 24 hours, set by default), monthly, quarterly, and annual gradations, seasonal, intra-season, and other gradations. The operator sets them based on the protected object's management decision. Theoretically, the number of gradations is not limited. Their choice determines all further work of the hardware and software complex on the formation and updating of the database and knowledge about the situational background of motor vehicles in the controlled area around the protected object.

It is necessary to enter into the database information about all MV object and their static and dynamic characteristics for the initial registration of vehicles. Forms of individual MV employees of near-object and transit transport enterprises are formed similarly. Thus, the data necessary for the start of the system (hardware and software complex) is accumulated. At the same time, more incomplete individual MV forms entering the system lead to faster adjustment.

The second procedure is the systematization of data about the situational background of MV in the controlled area around the protected object. It provides constant replenishment of the database by new individual vehicle forms. Of course, it may seem that this process is endless while the database volume should constantly increase. Eventually, the system will stop. However, modern hardware and software tools with relatively small dimensions can ensure the storage and use of large amounts of information (tens of millions of forms. The multitude of MVs operating near the objects of critical infrastructure is countable and much less than ten million.

The third procedure is the registration of violations and violators. The external surveillance data are constantly received from the video systems. They contain information about the static and dynamic characteristics of the MV that fall into the range of the video cameras. The received information is immediately compared with the parameters of vehicle characteristics stored in the database and knowledge (in individual MV forms). At least one discrepancy in the typical vehicle behavior is a deviation from the standard mode of its use or a violation of the 1st level. A vehicle that commits several violations is considered a violator. So, number of violations is much greater than the number of violators.

The fourth procedure is the identification of potential intruders. The main idea of detecting intruders is to register changes in their typical behavioral characteristics. Constant comparison of registered (new, from video systems) characteristics with the parameters in the database and knowledge only allows the identification of potential intruders. They can act unconsciously under particular circumstances and consciously understand what they are doing. Unfortunately, the system cannot conclude the intentions of potential violators. Operational workers take care of this.

The fifth procedure is a selection of influence on potential attackers performed by operative workers. The system, after a double rating selection of violators, issues a list of potential intruders in order of decreasing danger. Then, workers determine in what sequence, content, and how to work based on closed information at their disposal.

Preventive operative work allows the identification of new (previously unknown) characteristics of the vehicle, entering them into the database, and conducting preventive work with the violator if potential intruders act unconsciously under the influence of particular circumstances.

7 Conclusions

The developed mathematical model and information-technical method can be applied in the services of physical protection of critical infrastructure objects of Ukraine and strategic objects protected in the following five directions:

– process optimization to identify intruders in controlled zones around critical infrastructure objects in the interest of preventing emergency situations of a terrorist nature at the stages of planning and preparing terrorist acts against these objects;

– identification of potential gathering places of sabotage groups, hidden storages of weapons and ammunition and equipment;

– timely planning and effective implementation of operational measures to prevent terrorist acts at various stages of their preparation and implementation;

– development and creation of fundamentally new (intelligent) systems of protection and protection of protected objects;

– management of traffic flows on roads in cities and megacities.

References

1. 2016 Nice truck attack (2016) https://en.wikipedia.org/wiki/2016_Nice_truck_attack
2. Per Erik Gårder: Planning for Safe and Secure Transport Infrastructure. International Encyclopedia of Transportation. Elsevier. (2021). 418-425. https://doi.org/10.1016/B978-0-08-102671-7.10786-9
3. Faber, M.H., Stewart, M.G.: Risk assessment for civil engineering facilities: critical overview and discussion. Reliability Engineering & System Safety. Volume 80, Issue 2. (2003). 173-184. https://doi.org/10.1016/S0951-8320(03)00027-9
4. Stewart, M.G., Netherton, M.D.: Security risks and probabilistic risk assessment of glazing subject to explosive blast loading. Reliability Engineering & System Safety. 93(4) 627-638 (2008). https://doi.org/10.1016/j.ress.2007.03.007
5. Stewart, M.G.: Risk-informed decision support for assessing the costs and benefits of counter-terrorism protective measures for infrastructure. International Journal of Critical Infrastructure Protection. 3(1). 29-40 (2010). https://doi.org/10.1016/j.ijcip.2009.09.001
6. Semenets-Orlova, I., Rodchenko, L., Chernenko, I., Druz, O., Rudenko, M., Poliuliakii, R.: Requests for public information in the state Administration in situations of military operations. Ann. Fac. Der. U. Extremadura. 38. 249 (2022). https://doi.org/10.17398/2695-7728.38.249
7. Omar Elharrouss, Noor Almaadeed, Somaya Al-Maadeed. A review of video surveillance systems. Journal of Visual Communication and Image Representation. Volume 77. 103-116. (2021). https://doi.org/10.1016/j.jvcir.2021.103116
8. Taova, L.Yu.: Terrorism in transport is a threat to modern society. Theory and practice of social development. 12. 156-158. (2014).

9. Comprehensive Listing of Terrorism Victims in Israel. (2023). https://www.jewishvirtuallibrary.org/comprehensive-listing-of-terrorism-victims-in-israel
10. Terrorism and transport. (2023). https://www.unodc.org/unodc/en/terrorism/expertise/terrorism-and-transport.html
11. Daniel Dory, Tourism and international terrorism: a cartographic approach. Via. 19. (2021). https://doi.org/10.4000/viatourism.7243.
12. Al-Azzeh, J., Faure, E., Shcherba, A., Stupka, B.: Permutation-based frame synchronization method for data transmission systems with short packets. Egyptian Informatics Journal. 23(3). 529 – 545 (2022). https://doi.org/10.1016/j.eij.2022.05.005
13. Pospelov, B., Rybka, E., Krainiukov, O., Yashchenko, O., Bezuhla, Y., Bielai, S., Kochanov, E., Hryshko, S., Poltavski, E., Nepsha, O.: Short-term forecast of fire in the premises based on modification of the Brown's zero-order model. Eastern-European Journal of Enterprise Technologies, 4/10 (112), 52–58 (2021). https://doi.org/10.15587/1729-4061.2021.238555
14. Iatsyshyn A.V, Ivaschenko T.G., Matvieieva I.V., Zakharchenko J.V., Lahoiko A.M. Development of recommendations for improving the radiation monitoring system of Ukraine. IOP Conference Series: Earth and Environmental Science. 2023. Vol. 1254. 012109. https://doi.org/10.1088/1755-1315/1254/1/012109
15. Sadkovyi, V., Andronov, V., Semkiv, O., Kovalov, A., Rybka, E., Otrosh, Yu. et. al.; Sadkovyi, V., Rybka, E., Otrosh, Yu. (Eds.) Fire resistance of reinforced concrete and steel structures. Kharkiv: PC TECHNOLOGY CENTER, 180. (2021). https://doi.org/10.15587/978-617-7319-43-5
16. Diviziniuk, M., Farrakhov, O., Lysychenko, K., Zobenko, N., Bas, O.: Analysis of Radiation Background and Its Changes as Tool to Prevent Terrorist Emergencies at Critical Infrastructure Objects. In: Zaporozhets A., Popov O. (eds) Systems, Decision and Control in Energy IV. Volume II. Nuclear and Environmental Safety. Studies in Systems, Decision and Control. Vol. 456. 141-155. (2023). https://doi.org/10.1007/978-3-031-22500-0_9
17. Diviziniuk, M., Popov, O., Telelym, V., Kovach, V., Artemchuk, V.: General Characteristics of Radar Stations for Physical Protection of Nuclear Objects. In: Zaporozhets A., Popov O. (eds) Systems, Decision and Control in Energy IV. Volume II. Nuclear and Environmental Safety. Studies in Systems, Decision and Control. Vol. 456. 113-124. (2023). https://doi.org/10.1007/978-3-031-22500-0_7
18. Law of Ukraine. (2022). «About critical infrastructure». https://zakon.rada.gov.ua/laws/show/1882-20#Text
19. Law of Ukraine (2022) «On physical protection of nuclear installations, nuclear materials, radioactive waste, other sources of ionizing radiation». https://zakon.rada.gov.ua/laws/show/2064-14#Text
20. Alsayaydeh, J.A.J., Aziz, A., Rahman, A.I.A., Salim, S.N.S., Zainon, M., Baharudin, Z.A., Abbasi, M.I., Khang, A.W.Y.: Development of Programmable Home Security using GSM System for Early Prevention. ARPN Journal of Engineering and Applied Sciences. 16(1), 88 – 97 (2021). https://eprints.utem.edu.my/id/eprint/25751/2/JEAS_0121_8470.PDF

21. Otrosh, Y., Rybka, Y., Danilin, O., Zhuravskyi, M.: Assessment of the technical state and the possibility of its control for the further safe operation of building structures of mining facilities. E3S Web of Conferences, 123, 01012 (2019). https://doi.org/10.1051/e3sconf/201912301012
22. Abramov, Y., Basmanov, O., Salamov, J., Mikhayluk. A.: Model of thermal effect of fire within a dike on the oil tank. Naukovyi Visnyk Natsionalnoho Hirnychoho Universytetu,
23. Pospelov, B., Kovrehin, V., Rybka, E., et. al.: Development of a method for detecting dangerous states of polluted atmospheric air based on the current recurrence of the combined risk. Eastern-European Journal of Enterprise Technologies, 5/9 (107), 49–56 (2020). https://doi.org/10.15587/1729-4061.2020.213892 2, 95–100. (2018). https://doi.org/10.29202/nvngu/2018-2/12
24. Indha, W.A., Zamzam, N.S., Saptari, A., Alsayaydeh, J.A., Hassim, N.B.: Development of Security System Using Motion Sensor Powered by RF Energy Harvesting. In 2020 IEEE Student Conference on Research and Development, pp. 254 - 258 (2020) https://doi.org/10.1109/SCOReD50371.2020.9250984
25. The key task of our state and partners is to intensify Russia's feeling that it will not achieve anything in Ukraine - addressed by President Volodymyr Zelenskyy (2023). https://www.president.gov.ua/en/news/klyuchove-zavdannya-nashoyi-derzhavi-ta-nashih-partneriv-pos-80501