WEB ISSN 2535-0307
PRINT ISSN 1313-5031

TECHNICAL ASPECTS OF AUTOMATION OF TRANSPORT SECURITY

ТЕХНИЧЕСКИЕ АСПЕКТЫ АВТОМАТИЗАЦИИ ПРОЦЕДУР ОБЕСПЕЧЕНИЯ ТРАНСПОРТНОЙ БЕЗОПАСНОСТИ

Prof. Dr. Yelisov L.[1], Prof. Dr. Ovchenkov N.[2]
Moscow State Technical University of Civil Aviation, Moscow, Russia
lev.el@list.ru[1], ovchenkov@electronika.ru[2]

Abstract: *This research relates to air transport security and includes studies aimed at improving systems to ensure an acceptable level of transport security by solving technical challenges in the field of adaptive incident management.*

KEYWORDS: *TRANSPORT SECURITY, SECURITY SYSTEMS, ACCEPTABLE LEVEL, TECHNICAL CHALLENGES, ADAPTIVE INCIDENT MANAGEMENT*

1.Introduction

In recent years, the issue of air transport security has become of extreme importance given the unfavorable external conditions for activities related to transport services, such as the sharp rise in the number of illegal actions, including terrorism.

Professionals from different countries have been making significant efforts to solve this challenge and are increasingly creating specialized automated transport security systems. The most advanced achievements in various branches of science and technology are used as the technical basis for such systems.

Electronika Security Manager (ESM) is one such system. It was developed with the direct participation of the authors. ESM is a software and hardware platform that includes rather unique technical and organizational methodologies providing effective solutions for the entire complex of challenges related to securing the transport infrastructure. ESM was used as the foundation for the security system at Sochi Airport and demonstrated its effectiveness during the 2014 Winter Olympics.

2.1. Research Subject and Methods

ESM solves the entire range of tasks for managing facility security (see Fig. 1):

– Managing and integrating the facility's security subsystems – Collection and processing of data provided by different equipment and devices
– Alarm detection
– Assessment of the reliability and severity of alarms
– Identification of interrelated events and scenarios for the materialization of a particular threat
– Preliminary classification of incidents and deciding whether to assign incident status to the event – Initialization of the procedure for prompt response to the incident
– Collection of information on incidents; incident monitoring and management
– Ensuring the coordination of the Security Service and other departments
– Generation of alerts for senior managers to inform them of critical deviations
– Managing the enterprise security levels
– Real-time reporting
– Data distribution between users and convenient data presentation
– Automated submission of data on emergencies to law enforcement agencies

ESM includes the following subsystems: security alarm; alarm and warning system; process alarm; perimeter alarm; fire-safety systems; access control; video surveillance and video analysis; navigation satellite systems.

The system's interface is interactive and is designed to use state-of-the-art technology: video walls, stationary touch screens, tablets.

Alerters include the system's graphical interface, e-mail, texting, VoIP gateways connected to UTN/PBX, GSM, radio communications.

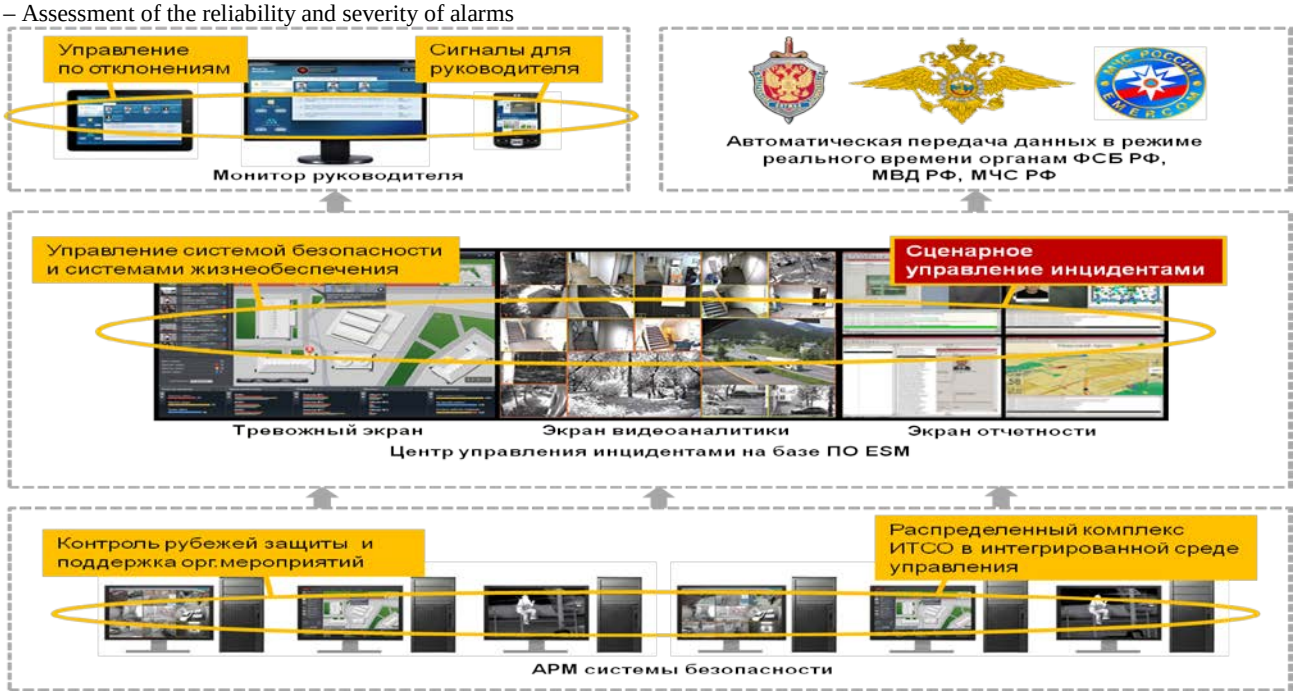

Figure 1. *Generalized structure of the ESM*

WEB ISSN 2535-0307
PRINT ISSN 1313-5031

The multicamera video analytics system can point a dome camera at an object and display people, vehicles, and other objects on the map in real time. Instant search for events in the archive using visual tools and the map; report generator with key video frames and descriptions. The monitoring system allows mobile objects to be monitored and tracked using GLONASS/GPS trackers.
The integrated radar-optical complex provides indiscriminate monitoring of the territory of the facility and restricted areas and also creates several virtual echeloned security lines. ONVIF is fully supported.

The video-surveillance system for the airport and landside is built on the basis of Milestone XProtect Corporate. This is one of the most powerful software products in the world that supports an unlimited number of servers, cameras, users, and virtually all vendors. This solution provides centralized management for all devices, servers, and users and also supports flexible rules with time-based and event-based triggers. This system includes the following components: system management server combined with SQL Express; Milestone recording servers; storage servers; AgentVI analytical servers; Milestone workstations (see Figure 2).

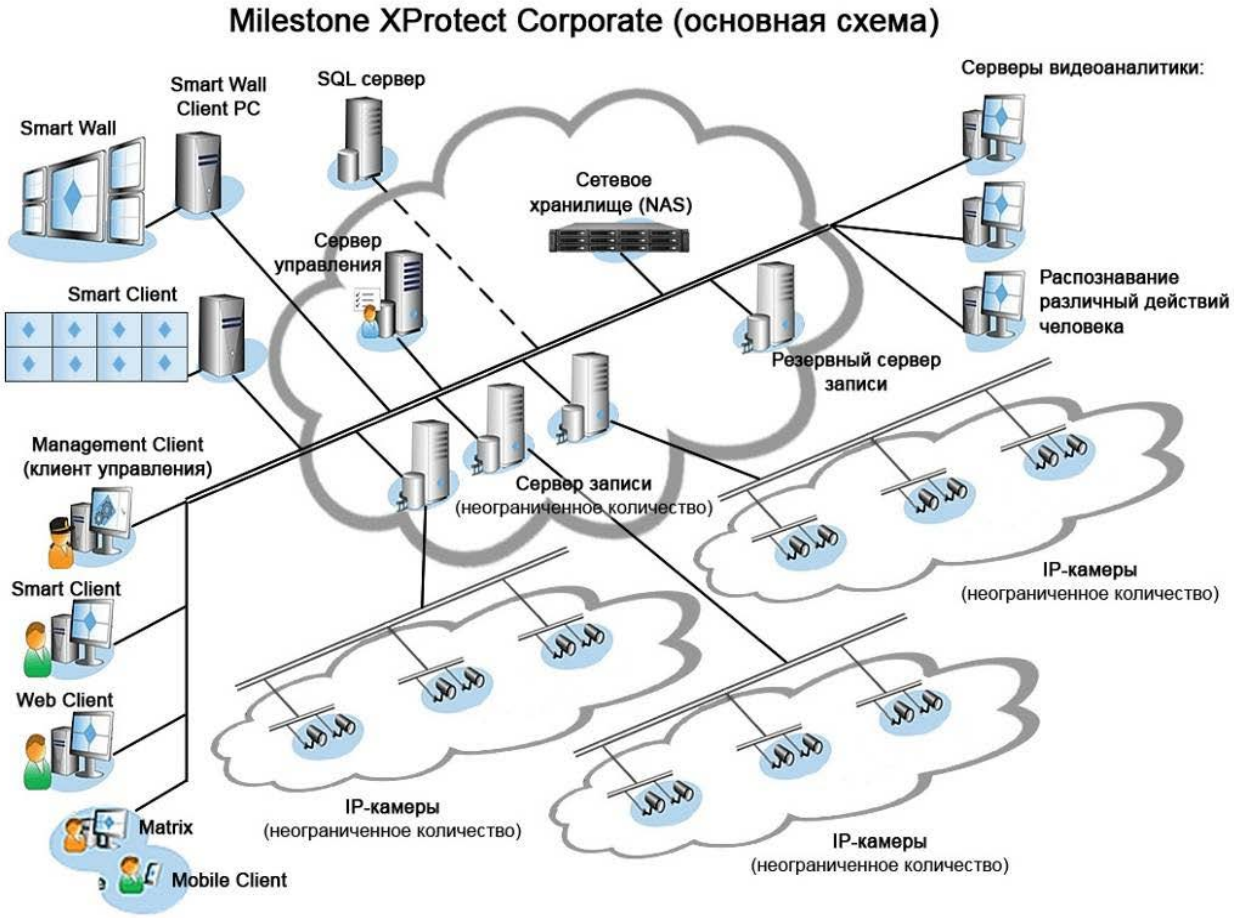

Figure 2. *Structure of the Milestone XProtect Corporate solution*

The video-analytics system uses Agent VI software in conjunction with Milestone XProtect. Agent VI is a platform for managing video analytics. The Data Collection and Processing System (DCPS) consists of a server based on ESM-server software and automated workstations based on ESM-client software.

The Transport Security Command Console (TSCC) is the central guard post for centralized output of information to digital monitors. The TSCC has operational control capabilities covering all the subsystems of the airport's Technical Security Equipment Set (TSES) (see Figure 3). The TSCC consists of several Automated Workstations (AWS). The centralized information environment and a single database enable a unified approach to information collection and processing. The interfaces were designed taking into account the goals and tasks of each user role.

Electronika Security Manager is a software platform deploying a single complex based on different equipment, devices, and software.

WEB ISSN 2535-0307
PRINT ISSN 1313-5031

Figure 3. *Transport Security Command Console*

The integrated engineering safety systems and security alarm provide the following options: automatic response to an intruder attempting to enter a protected area and/or perimeter section, prompt notification of security personnel, and ensuring coordination of their actions.

Integration with the Intellect video-surveillance system provides the following capabilities: monitoring and control of video cameras, servers, video monitors; importing photos and events from Intellect; displaying video signals taking into account actuated alarm-initiating devices; analysis of archived alarms in the ESM-client interface; monitoring of events triggered by video-analytics sensors.

Integration with the Milestone XProtect video-surveillance system provides the following capabilities: receive and save XProtect alarms in the ESM database; put XProtect alarms on the list of alarm events; obtain the time of the beginning of the alarm event from the video archive and save it in the nESM database to be able to view video recordings associated with this event; put alarms of the AgentVI video analytics on the list of ESM alarm events; display video signals from all cameras associated with the alarm on the alarm monitor in real time; obtain the time of the beginning of the alarm event from the video archive and save it in the database; execute commands bound to the alarm.

Integration of existing security systems that are based on BIS (BOSCH) software provides the following features: centralized creation and management of users in BIS; centralized creation and management of access cards in BIS; centralized import of the list of access rights from BIS to ESM; centralized assignment of access rights and access cards to users in BIS; centralized management of access cards (activation and deactivation) and BOSCH equipment from BIS; centralized removal of access rights and access cards in BIS; centralized export of events related to users entering protected facilities in BIS; centralized export of events related to denial of user access to protected facilities in BIS; export of the list of access zones from BIS to correctly decipher events related to user access.

ESM provides step-by-step instructions for operators on responding to alarms and adjusts them taking into account the dynamics of negative impacts (see Figure 4). This approach increases response speed and accuracy, reduces requirements regarding the level of operator training, makes the situation more controllable, and increases the effectiveness of the measures taken. The response algorithm consists of the following three stages: receiving an alarm, verifying it, and executing the instructions.

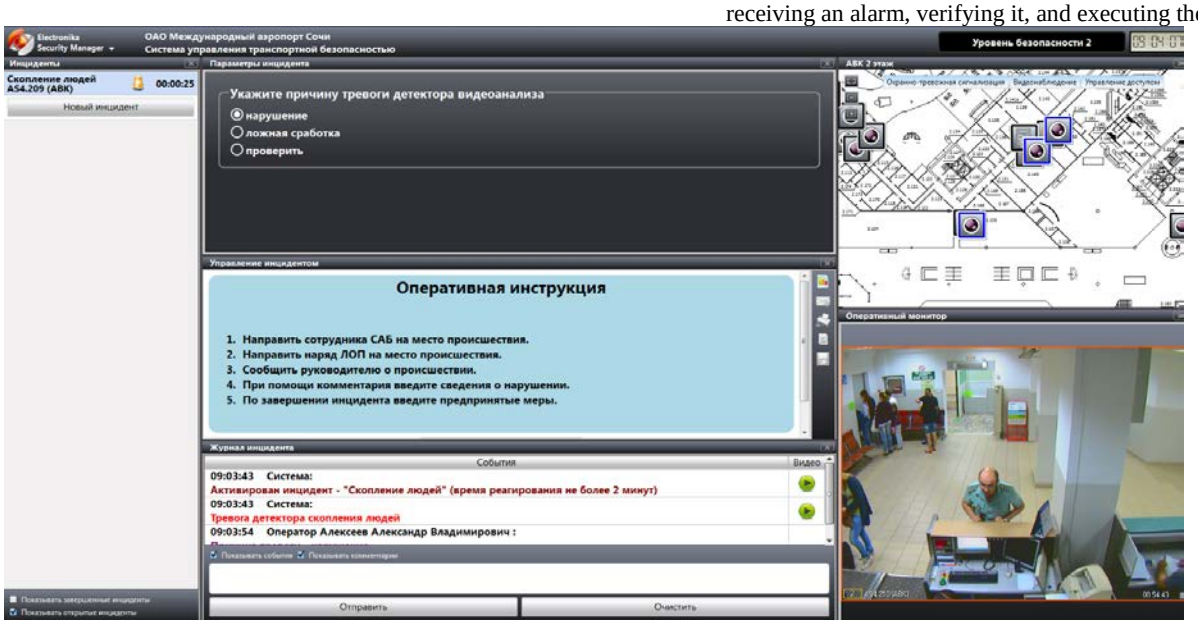

Figure 4. *Operating instructions*

WEB ISSN 2535-0307
PRINT ISSN 1313-5031

The operating instructions include: malfunction of equipment or devices, security-system alarm, alarm-system alarm, people running in a controlled area, vehicles in the controlled area for too long, a large number of people in the controlled area, vehicles going too fast in the controlled area, activated Antipanic mode at the checkpoint, manual access control at the checkpoint.

Automated management of responses to incidents that are treated as groups of events obtained from different subsystems and correlated with one incident. In this case, comparison criteria (time and place of the incident) are taken into account. The system contains the following types of incidents: incidents related to alarms and incidents related to user access. Each incident can have three states: active, inactive, closed (see Figure 5).

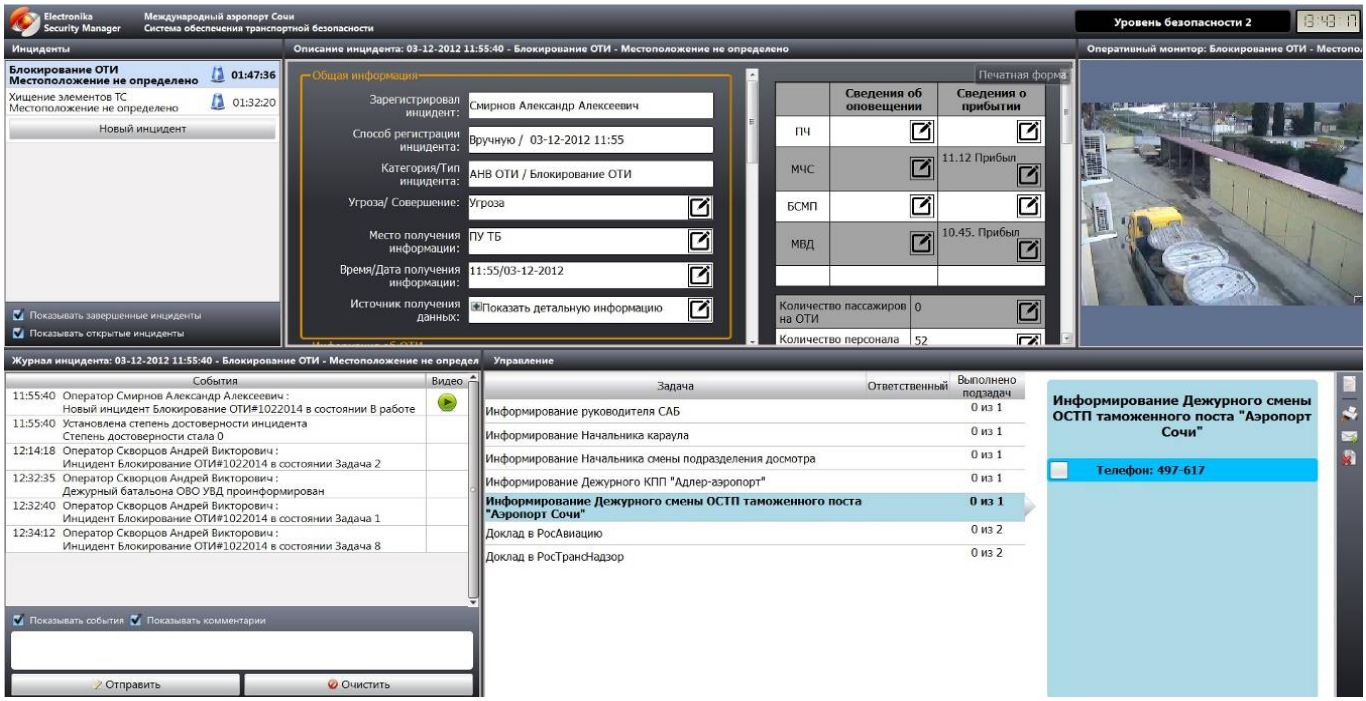

Figure 5. *Incident management*

Incident management is reduced to the operator processing alarm events. These events are triggered by security systems in accordance with the incident model implemented in ESM. Alarm events may be associated with activated security alarms, unclosed doors, pressed emergency buttons, suspicious objects in the surveillance area of the video camera, or activated detectors of the video camera. After processing the incidents, the necessary information for an Act of Unlawful Interference (AUI) is gathered, and AUI reports are generated for the competent authorities.

2.Conclusion

The proposed technical solutions implementing the methods for dynamic integration of transport-security systems at the airport are based on principles that imply that these technical solutions are a single dispersed system with a reconfigurable structure. Technical solutions related to integration management are based on the concept of object vulnerability, which is considered a qualitative characteristic. The set of security equipment and systems must be adequate for the level of vulnerability expressed as the quality of the systems for ensuring transport security. The control parameter expressed in quantitative terms is determined using qualimetry. The proposed technical solutions implement all necessary data connections to ensure proper management within the transport security system and solve tasks related to the dynamic integration of security systems at the airport.

Bibliography

1. L. N. Yelisov, N. I. Ovchenkov, R. S. Fadeyev. Introduction to aviation security. Monograph (Ed. by Professor L. N. Yelisov), Yaroslavl: Filigran, 2016, 320 p.
2. L. N. Yelisov. Qualitative procedures for integrating radio-security equipment at the airport] / L. N. Yelisov, N. I. Ovchenkov // Scientific Bulletin of the MSTUCA, Moscow: MSTUCA, 2012, No. 186, pp. 138–142.
3. L. N. Yelisov. On some classes of optimization problems being solved using informal methods / L. N. Yelisov, S. V. Gromov, N. I. Ovchenkov // Scientific Bulletin of the MSTUCA, Moscow: MSTUCA, 2012, No. 186, pp. 130–135.
4. L. N. Yelisov Assessment of the vulnerability of transport infrastructure and aircraft in civil aviation / N. I. Ovchenkov, L. N. Yelisov // Scientific Bulletin of the MSTUCA, Moscow: MSTUCA, 2014, No. 204, pp. 65–68.