SECOND HIGH-LEVEL CONFERENCE ON AVIATION SECURITY (HLCAS/2)

Montréal, 29 to 30 November 2018

Agenda Item 3: Global Aviation Security Plan

INNOVATIVE TECHNOLOGY OF INTEGRATION AND CONTROL OF INFORMATION FLOWS ON SECURITY AT THE AIRPORT TO IMPROVE THE EFFICIENCY OF THE AVIATION SECURITY MANAGEMENT SYSTEM

(Presented by the Russian Federation)

SUMMARY

This document contains material relating to proposals for the use of innovative technology that can significantly improve the level of aviation security, ensuring control over all information flows at the airport, while minimizing the impact of the human factor (operator) on aviation security, as well as providing for the implementation of the task of PD 3.2 and 3.3 of the Roadmap for the implementation of the ICAO Global Aviation Security Plan (GASeP).

Action by the High-level Conference on Aviation Security is in paragraph 5.

1.   **INTRODUCTION**

1.1   On 19-21 October 2016, during the 3rd meeting of the Aviation Security Panel Working Group on Innovation in Aviation Security in Singapore, the Russian Federation presented a document on the development of a unique technology for the construction of an aviation security system «Electronic Security Management System (ESpsM)». It enables integration of information flows from the subsystems of the airport security and in a timely manner to identify threats. The document was of great interest and was supported by the participants of the meeting.

1.2   When discussing the document, the Meeting (international experts of the work group) pointed out high efficiency of that kind of systems for the fact that such technologies monitor all airport information flows, while minimizing the impact of the operator, the human factor, on the aviation security management in the airport.

1.3   In the Report of the 5th meeting of the Aviation Security Regional Group – Europe and North Atlantic, held from 24-26 May 2016 in Paris, following the review of this innovation, the Group's experts called for the use of this type of technology to improve the efficiency and strengthen the aviation security management system, and recommended the use of this type of technology, given that this type of innovation can reduce the risks of wrong decisions in the face of lack of time and incomplete information in the event of a threat of acts of unlawful interference.

---

[1] English and Russian versions provided by the Russian Federation.

1.4   In accordance with Annex 17 to the Convention on International Civil Aviation, in order to achieve the objectives of civil aviation security, each contracting state is encouraged, where necessary and to the extent practicable from an operational, technical and financial point of view, to use technical means of security and to take into account human aspects.

2.   SPECIAL TECHNOLOGY OF THE INFORMATION FLOWS INTEGRATION

2.1   In the Russian Federation, at the national and at the airport levels, there are measures set to upgrade existing technologies and procedures, as well as to develop innovative solutions in building up effective aviation security system.

2.2   Following up on the legislative requirement there is *Electronic Security Management System* (ESpsM), a unique technology designed in the Russian Federation to build up aviation security. It provides for the integration of the information feeds from the security subsystems of the facility, early detection of threats, management of all response phases, analysis of the efficacy of the response measures and monitoring operator's actions to ensure compliance with the active security operating procedures. This technology can be adapted to the needs of a specific airport.

2.3   In the Russian Federation the ESpsM technology is implemented in the *Electronika Security Manager* software. First time the system was commissioned and has since proven its efficacy in the airports of Sochi, Krasnodar and Anapa in the period of the 2014 Winter Olympic Games. At present, application of the *Electronika Security Manager* is rolled out in the other airports in the Russian Federation.

3.   AUTOMATION OF THE COMPLEX ANALYSIS AND RESPONSE TO A THREAT

3.1   *Electronika Security Manager* integrates information flows from the airport security subsystems into a single platform and controls the entire airport area: it receives alert, evaluates severity of the threat, selects counteraction scenario, tracks results of the incident and evaluates efficacy of the response measures.

3.2   *Electronika Security Manager* supports open and standard protocols to make use of the existing security systems on the facility and ensure their seamless connectivity with the new complex, quick retrofitting and upgrading with the latest technical means and technologies.

3.3   *Electronika Security Manager* complements the system of continuous monitoring of aviation security with emergency response control functions:

> a) listings of the security incidents and listings of the standard response scenarios;
>
> b) a complex approach, which Electronika Security Manager is based on, combines methodological (regulations, instructions), technical (security systems equipment) and organizational (human resources) components in one solution and enables general management of security policies, automatically increase/decrease security level to adjust to the threat level change; and
>
> c) to choose optimal strategy of responding to various types of incidents, on the state level, in the framework of the system of continuous monitoring of the aviation security, there is   a need for the expertise of the emergency response process (workplaces for experts and the expert portal for external experts got to be created).

3.4   *Electronika Security Manager* tracks related events by matching information from different sources, and combines a sequence of events of the same incident in an incident card.

3.5   *Electronika Security Manager* assesses the credibility of the information through complex analysis of signals from different sources (technical detectors, motion video detectors, situational video analysers, weather reports, information from the technical security operators on the verification of video surveillance data or messages from the emergency response team).

3.6   Credibility of the information influences the way the information is displayed, and the operator response options to the alert. On the events with the average credibility and above, *Electronika Security Manager* automatically activates step-by-step instructions on how to resolve the incident, and an operator is not able to dismiss them without responding. Events of the less than average credibility are displayed in the form of video windows with decision buttons of the "Alarm", "False alarm" and "Verification Required". Incident mode is activated following the operator decision, while information sufficient to assess efficacy of the response action is stored into the system.

3.7   *Electronika Security Manager* exposes operator mistakes in assessing particular alerts and in responding to the incident as a whole.

3.8   *Electronika Security Manager* features a capability to carry out contingency action plan training.

4.   **CONCLUSIONS**

4.1   Such systems as *Electronika Security Manager* allow for the significant raise of the aviation security level, providing control of all airport information flows, while minimizing the impact of the human factor/operator on the aviation security management in the airport.

5.   **ACTION BY THE HIGH-LEVEL CONFERENCE**

5.1   The High-level Conference on Aviation Security is invited to:

   a) note the content of the information about the innovative technology of integration and control of information flows on aviation security at the airport applied in the Russian Federation for improvement of the effective system of management of aviation security;

   b) encourage the ICAO Secretariat to pay attention to the need to expand the functionality of the AVSECPaedia platform, so that States can exchange experience, including on the aviation security information systems used;

   c) encourage the ICAO Secretariat to consider the proposal for the addition in paragraph 11.2.1 of the Aviation Security Manual (Doc 8973/9) the subparagraph e) to recommend the use of the software type «Electronika Security Manager», able to provide continuous monitoring and information integration of all subsystems of the airport security and is able to manage all phases of response and monitoring the effectiveness of measures taken; and

   d) agree the need to continue work in this area.

— END —