



РАБОЧИЙ ДОКУМЕНТ

ВТОРАЯ КОНФЕРЕНЦИЯ ВЫСОКОГО УРОВНЯ ПО АВИАЦИОННОЙ БЕЗОПАСНОСТИ (HLCAS/2)

Монреаль, 29–30 ноября 2018 года

Пункт 3 повестки дня. Глобальный план обеспечения авиационной безопасности (ГПAB)

ИННОВАЦИОННАЯ ТЕХНОЛОГИЯ ИНТЕГРАЦИИ И КОНТРОЛЯ ИНФОРМАЦИОННЫХ ПОТОКОВ ПО БЕЗОПАСНОСТИ В АЭРОПОРТУ ДЛЯ ПОВЫШЕНИЯ ЭФФЕКТИВНОСТИ СИСТЕМЫ УПРАВЛЕНИЯ АВИАЦИОННОЙ БЕЗОПАСНОСТЬЮ

(Представлено Российской Федерацией)

АННОТАЦИЯ

В настоящем документе содержится материал, касающийся предложений об использовании инновационной технологии, позволяющей существенно повысить уровень обеспечения авиационной безопасности, обеспечивая контроль за всеми информационными потоками в аэропорту, при этом минимизируя влияние человеческого фактора (оператора) на обеспечение авиационной безопасности, а также предусматривающей реализацию задачи ПД 3.2 и 3.3 Дорожной карты реализации Глобального плана обеспечения авиационной безопасности ИКАО.

Действия Конференции высокого уровня по авиационной безопасности указаны в п. 5.

1. ВВЕДЕНИЕ

1.1 19–21 октября 2016 года в ходе 3-го Совещания Группы по инновациям в области авиационной безопасности в Сингапуре Российская Федерация представила документ в отношении разработки уникальной технологии для построения системы авиационной безопасности "Электронная система управления безопасностью (ESpsM)". Она обеспечивает интеграцию информационных потоков от подсистем безопасности аэропорта и своевременно выявляет угрозы. Представленный документ вызвал высокий интерес и нашел поддержку участников совещания.

1.2 При обсуждении документа участники совещания (эксперты рабочей группы разных государств) отметили высокую эффективность такого рода систем в силу того, что

¹ Документ на русском и английском языках представлен Российской Федерацией.

подобные технологии обеспечивают контроль за всеми информационными потоками в аэропорту, при этом минимизируя влияние человеческого фактора (оператора) на обеспечение авиационной безопасности в конкретном аэропорту.

1.3 В отчете 5-го совещания Региональной группы по авиационной безопасности – Европа и Северная Атлантика, проходившего 24–26 мая 2016 года в г. Париж, по результатам рассмотрения данной инновации эксперты Группы призвали применять такого рода технологии для повышения эффективности и усиления системы управления авиационной безопасностью, а также рекомендовали использовать такого рода технологии с учетом того, что данного типа инновации позволяют снизить риски неправильных решений в условиях дефицита времени и неполной информации в случае возникновения угрозы актов незаконного вмешательства.

1.4 В соответствии с Приложением 17 к Конвенции о международной гражданской авиации для достижения целей безопасности гражданской авиации каждому Договаривающемуся государству рекомендуется там, где это необходимо, и в той мере, в какой это практически возможно с эксплуатационной, технической и финансовой точек зрения, использовать технические средства обеспечения и учитывать аспекты человеческого фактора.

2. СПЕЦИАЛЬНАЯ ТЕХНОЛОГИЯ ИНТЕГРАЦИИ ИНФОРМАЦИОННЫХ ПОТОКОВ

2.1 В Российской Федерации на национальном и аэропортовом уровне реализуется комплекс мер по совершенствованию действующих технологий и процедур, а также разработке инновационных решений, направленных на создание эффективно функционирующей системы авиационной безопасности.

2.2 В связи с этим в Российской Федерации разработана специальная технология для построения системы авиационной безопасности "*Электронная система управления безопасностью (ESpsM)*". Она обеспечивает интеграцию информационных потоков от подсистем безопасности объекта, своевременное выявление угроз, управление всеми этапами реагирования, анализ эффективности предпринятых мер и контроль действий оператора на предмет соответствия действующим требованиям безопасности. Данную технологию возможно адаптировать к требованиям конкретного аэропорта.

2.3 В Российской Федерации технология ESpsM реализована в программном обеспечении "*Electronika Security Manager*". Система впервые была внедрена и показала свою эффективность в аэропортах Сочи, Краснодара и Анапы в период проведения Зимних Олимпийских игр в России. В настоящее время продолжается работа по расширению применения системы "*Electronika Security Manager*" в аэропорты Российской Федерации.

3. АВТОМАТИЗАЦИЯ КОМПЛЕКСНОГО АНАЛИЗА И РЕАГИРОВАНИЯ НА УГРОЗУ

3.1 "*Electronika Security Manager*" интегрирует информационные потоки от подсистем безопасности аэропорта в единый комплекс и управляет ситуацией в масштабах всего аэропорта: позволяет оперативно получить сигнал, оценить критичность угрозы, выбрать сценарий противодействия, отследить результаты инцидента и оценить эффективность предпринятых действий.

3.2 *"Electronika Security Manager"* обеспечивает поддержку открытых и стандартных протоколов с целью сохранения уже имеющихся на объекте систем безопасности, обеспечения беспрепятственного подключения их к новому комплексу систем, оперативного развития и модернизации, подключения новейших технических средств и технологий.

3.3 *"Electronika Security Manager"* дополняет Систему непрерывного мониторинга уровня авиационной безопасности функциями управления процессом реагирования на внештатные ситуации:

- a) предусмотрены перечни инцидентов безопасности и типовых сценариев реагирования на них;
- b) комплексный подход, заложенный в основу «Electronika Security Manager» и сочетающий в одном решении методологические (регламенты, инструкции), технические (оборудование систем безопасности) и организационные (человеческие ресурсы) компоненты позволяет осуществлять общее управление политикой безопасности, в автоматическом режиме повышать/понижать уровень безопасности при изменении уровня угрозы;
- c) с целью выбора оптимальной стратегии реагирования на разные виды инцидентов на уровне государства в рамках системы непрерывного мониторинга уровня авиационной безопасности необходима экспертиза хода реагирования на критические инциденты (создание рабочих мест экспертов и экспертного портала для внешних экспертов).

3.4 *"Electronika Security Manager"* отслеживает взаимосвязанные события путем сопоставления информации из разных источников и объединяет последовательности событий, принадлежащих одной ситуации в учетную карточку инцидента.

3.5 *"Electronika Security Manager"* обеспечивает оценку достоверности информации путем комплексного анализа сигналов от различных источников (сигналы от технических средств обнаружения, сигналы от видеодетекторов движения и средств ситуационного видеоанализа, информация о погодных условиях с метеостанции, информация от оператора технических средств охраны о подтверждении или опровержении информации, полученной с использованием средств видеонаблюдения, или сообщений от группы быстрого реагирования).

3.6 Достоверность информации влияет на вид отображаемой информации и возможности оператора по реагированию на данную тревогу. По событиям, имеющим достоверность от средней и выше, *"Electronika Security Manager"* автоматически активирует запуск пошаговых инструкций по разрешению инцидентов, оператор не имеет возможности их сбросить без реагирования. События с достоверностью ниже средней отображаются в виде видеоокна с кнопками принятия решения "Тревога", "Ложная тревога", "Требуется проверка". Активация инцидента производится в зависимости от принятого оператором решения, при этом сохраняется информация, достаточная для проверки правильности принятого решения.

3.7 *"Electronika Security Manager"* выявляет ошибки персонала, допущенные при оценке отдельных тревожных сигналов и в реагировании на инцидент в целом.

3.8 *"Electronika Security Manager"* предоставляет возможность проведения учебной отработки плана действий на случай непредвиденных обстоятельств.

4. **ВЫВОДЫ**

4.1 Системы типа "*Electronika Security Manager*" позволяют существенно повысить эффективность управления авиационной безопасностью, обеспечивая интеграцию и контроль за всеми информационными потоками в аэропорту, при этом минимизируя влияние человеческого фактора (оператора) на обеспечение авиационной безопасности в конкретном аэропорту.

5. **ДЕЙСТВИЯ КОНФЕРЕНЦИИ ВЫСОКОГО УРОВНЯ**

5.1 Конференции высокого уровня по авиационной безопасности предлагается:

- a) принять к сведению информацию о применяемой в Российской Федерации инновационной технологии интеграции и контроля информационных потоков по безопасности в аэропорту для повышения эффективной системы управления авиационной безопасностью;
- b) призвать Секретариат ИКАО обратить внимание на необходимость расширения функциональности платформы AVSECPaedia, с тем, чтобы государства-участники могли обмениваться опытом в том числе и по используемым информационным системам по авиационной безопасности;
- c) призвать Секретариат ИКАО рассмотреть предложение о дополнении Руководства по авиационной безопасности (Doc 8973/9) в п. 11.2.1 главы 11 "Безопасность аэропорта" подпунктом e) рекомендовать использование программного обеспечения типа "Electronika Security Manager", способного обеспечить непрерывный мониторинг и интеграцию информации всех подсистем безопасности аэропорта и способного управлять всеми этапами реагирования и контроля эффективности принятых мер.
- d) согласиться с необходимостью продолжения работы в указанном направлении.

— КОНЕЦ —