Международные требования к информационной безопасности в аэропортах

Международный аэропорт Петрозаводск

Иванов Эдуард

Правовая основа

Российское законодательство

Федеральный закон № 16-ФЗ «О транспортной безопасности» в редакции Федерального закона от 03.04.2023 № 107-ФЗ «О внесении изменений в Федеральный закон «О транспортной безопасности» и отдельные законодательные акты Российской Федерации» (вступает в силу с 01.03.2024)

Обеспечение транспортной безопасности на объектах транспортной инфраструктуры и транспортных средствах воздушного транспорта включает в себя осуществление комплекса мер по обеспечению защиты гражданской авиации от актов незаконного вмешательства, который предусмотрен стандартами Международной организации гражданской авиации в области защиты гражданской авиации от актов незаконного вмешательства.;

Международное законодательство

DOC ICAO

РУКОВОДСТВО ПО АВИАЦИОННОЙ БЕЗОПАСНОСТИ

ГЛАВА 18

КИБЕРУГРОЗЫ КРИТИЧЕСКИ ВАЖНЫМ АВИАЦИОННЫМ СИСТЕМАМ ИНФОРМАЦИОННЫХ И СВЯЗНЫХ ТЕХНОЛОГИЙ

Стандарты ICAO

Меры, касающиеся киберугроз

4.9.1 Каждое Договаривающееся государство обеспечивает, чтобы эксплуатанты или организации, указанные в национальной программе безопасности гражданской авиации или другой соответствующей национальной документации, определяли свои критически важные системы информационных и связных технологий и данные, используемые для целей гражданской авиации, и в соответствии с оценкой риска разрабатывали и внедряли, по мере необходимости, меры их защиты от незаконного вмешательства.

4.9.2 Рекомендация. Каждому Договаривающемуся государству следует обеспечивать, чтобы реализуемые меры защищали, по мере необходимости, конфиденциальность, целостность и готовность определяемых критически важных систем и/или данных. Указанные меры должны предусматривать, по мере необходимости и в
соответствии с оценкой риска, проводимой его соответствующими национальными полномочными органами, в
частности, учет аспектов безопасности на этапе разработки, обеспечение безопасности цепи поставок, разделение
сетей и защиту и/или ограничение любых возможностей дистанционного доступа.

Обзор поправок в документы ICAO по киберугроз

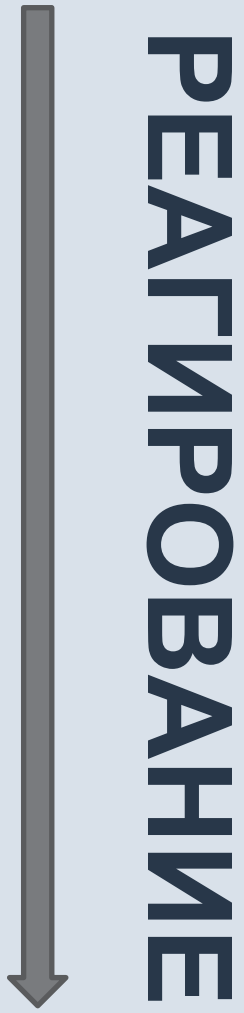
Поправка	Источник(и)	Вопрос(ы)	Даты принятия, вступления в силу, начала применения
12 (9-издание)	Предложения Комитета по незаконному вмешательству, подготовленные при содействии Группы экспертов по авиационной безопасности (AVSECP), и действия Совета, предпринятые во исполнение резолюции A36-20 Ассамблеи	Данная поправка включает в себя положения, предусматривающие дальнейшее усиление Стандартов и Рекомендуемой практики в целях устранения новых и возникающих угроз гражданской авиации. Поправка включает следующее: размещение технических средств обеспечения безопасности; обеспечение безопасности поставщиков обслуживания воздушного движения; программы подготовки кадров и система сертификации инструкторов; выборочные и непредсказуемые меры безопасности; безопасность цепи поставок; безопасность в отношении всех полетов грузовых воздушных судов; киберугрозы; и определения	17 ноября 2010 г. 26 марта 2011 г. 1 июля 2011 г.

	(WGA17)	четкости изменена редакция существующих положений, касающихся проведения оценок риска и мер защиты от киберугроз	
16	Предложения 28-го совеща- ния Группы экспертов по авиационной безопасности (AVSECP/28), подготовленные при содействии Рабочей группы по Приложению 17 (WGA17)	Данная поправка включает в себя ссылку на учебные комплекты по авиационной безопасности. Она также включает в себя новые/пересмотренные положения, касающиеся обмена информацией, мер в отношении пассажиров и ручной клади, мер, касающихся груза, почты и других предметов и киберугроз	14 марта 2018 г. 16 июля 2018 г. 16 ноября 2018 г.

Эксплуатантам следует разработать план реагирования на происшествия в области кибербезопасности, в котором описывается организационный подход к реагированию на кибератаку, в том числе действия, предпринимаемые техническими, правовыми, отвечающими за техническое обслуживание, за связь с общественностью и прочими организационными подразделениями, участвующими в процессе снижения уровня риска кибератак и противодействия им. План реагирования на происшествия в области кибербезопасности должен включать подробное и всеобъемлющее описание действий по поддержанию непрерывной деятельности, которые осуществляются в том случае, если одна или несколько систем, считающихся критически важными, становятся недоступными или ненадежными.

Подобный план должен включать следующее:

- a) методику классификации для определения серьезности инцидента, с тем чтобы можно было принять соответствующие меры реагирования;
- b) оперативное решение, разработанное с целью гарантировать непрерывное и безопасное управление находящимся в воздухе воздушным судном, воздушным пространством или аэропортом, которых коснулся инцидент;
- c) план обеспечения непрерывности обслуживания с инструкциями о том, как восстановить работу данных систем в штатном режиме в течение определенного времени восстановления или, если безопасное и соответствующее восстановление работы систем невозможно, план продолжения деятельности с использованием для этого других средств;
- d) план, обеспечивающий невозможность дальнейшего использования выявленных уязвимых мест в целях создания угрозы безопасности пассажиров, экипажа и наземного персонала;
- e) план восстановления в чрезвычайных ситуациях для возобновления работы в полном объеме;
- f) план уведомления об аварийной ситуации всех заинтересованных сторон, сотрудников и государств, с тем чтобы максимально оперативно обеспечить наличие персонала, необходимого для восстановления обслуживания, и предоставить ключевую информацию всем соответствующим партнерам.



РЕАГИРОВАНИЕ

План связи в кризисной ситуации

18.2.5.1 Государствам и отрасли следует сотрудничать с их соответствующими организациями, с тем чтобы обеспечить наличие планов связи в кризисной ситуации для эффективной и оперативной связи с заинтересованными сторонами и общественностью при реагировании на инциденты в области кибербезопасности.

18.2.5.2 План связи в кризисной ситуации может включать:

- a) определение вероятных сценариев инцидентов в области кибербезопасности и соответствующих планов действий;
- b) определение целевой аудитории и заинтересованных сторон для каждого из сценариев инцидентов в области кибербезопасности;
- c) выбор основного(ых) пресс-секретаря(ей) и технических экспертов, которые будут представлять организацию и общаться со СМИ;
- d) определение соответствующих платформ/каналов для информационно-разъяснительной работы (традиционные СМИ, социальные сети и т. д.);
- e) формирование группы информационной поддержки в кризисных ситуациях, которая начинает функционировать в случае кризиса.

Спасибо за внимание!

Иванов Эдуард Борисович
Руководитель ПТАБ
БУ РК «Аэропорт @Петрозаводск»
Telegram 89535267353
89658171902
sab@karelavia.ru