ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 57240—2016

Воздушный транспорт

МЕНЕДЖМЕНТ БЕЗОПАСНОСТИ АВИАЦИОННОЙ ДЕЯТЕЛЬНОСТИ В ГРАЖДАНСКОЙ АВИАЦИИ

Основные положения

Издание официальное

Москва
Стандартинформ
2016

дезарт-совместно

Предисловие

1 РАЗРАБОТАН федеральным государственным бюджетным образовательным учреждением высшего образования «Московский государственный технический университет гражданской авиации» (МГТУ ГА)

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 034 «Воздушный транспорт»

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 9 ноября 2016 г. № 1630-ст

4 ВВЕДЕН ВПЕРВЫЕ

Правила применения настоящего стандарта установлены в статье 26 Федерального закона «О стандартизации в Российской Федерации». Информация об изменениях к настоящему стандарту публикуется в ежегодном (по состоянию на 1 января текущего года) информационном указателе «Национальные стандарты», а официальный текст изменений и поправок — в ежемесячном информационном указателе «Национальные стандарты». В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ближайшем выпуске ежемесячного информационного указателя «Национальные стандарты». Соответствующая информация, уведомление и тексты размещаются в информационной системе общего пользования — на официальном сайте Федерального агентста по техническому регулированию и метрологии в сети Интернет (www.gost.ru)

© Стандартинформ, 2016

Настоящий стандарт не может быть полностью или частично воспроизведен, тиражирован и распространен в качестве официального издания без разрешения Федерального агентства по техническому регулированию и метрологии

Содержание

1 Область применения . . . 1
2 Нормативные ссылки . . . 1
3 Сокращения, термины и определения . . . 2
3.1 Сокращения . . . 2
3.2 Термины и определения . . . 2
4 Общая характеристика менеджмента безопасности авиационной деятельности с учетом контекста организации . . . 4
4.1 Компоненты менеджмента безопасности организации — поставщика обслуживания . . . 4
4.2 Область действия системы менеджмента безопасности авиационной деятельности . . . 4
5 Требования к системе менеджмента безопасности авиационной деятельности . . . 5
5.1 Общие требования . . . 5
5.2 Обязательства и ответственность руководства . . . 6
5.3 Политика в области безопасности авиационной деятельности . . . 6
5.4 Культура безопасности . . . 6
5.5 Риск-менеджмент безопасности авиационной деятельности . . . 6
5.6 Определение критериев и показателей эффективности функционирования СМБАД . . . 8
5.7 Осуществление изменений . . . 8
6 Требования к процессам управления аспектами безопасности авиационной деятельности . . . 8
6.1 Управление безопасностью полетов . . . 8
6.2 Требования к управлению авиационной безопасностью . . . 10
6.3 Требования к управлению экологической безопасностью авиационной деятельности поставщиков обслуживания . . . 11
6.4 Требования к управлению производственной безопасностью поставщика обслуживания . . . 12
6.5 Управление информационной безопасностью . . . 13
Библиография . . . 16

Введение

Безопасность является важнейшим свойством и характеристикой авиационной деятельности и включает следующие аспекты:

- безопасность полетов;
- авиационную безопасность;
- экологическую безопасность;
- производственную безопасность.
- информационную безопасность.

Соответственно, система менеджмента безопасности авиационной деятельности (СМБАД) должна включать процедуры и методы управления по всем аспектам безопасности.

Безопасность полетов является центральным аспектом безопасности авиационной деятельности. Вопросы безопасности полетов составляют основное содержание стандартов и рекомендуемой практики (SARPs) Международной организации гражданской авиации (ИКАО), содержащихся в ряде приложений к Конвенции о международной гражданской авиации 1944 г. В настоящее время вопросы управления безопасностью в наибольшей степени проработаны именно в части управления безопасностью полетов как на государственном уровне, так и на уровне поставщиков обслуживания. Государство взяло на себя обязанности по выполнению SARPs, относящихся к управлению безопасностью полетов. Тем ни менее, процедуры разработки и внедрения программ и систем управления безопасностью полетов нуждаются в стандартизации.

Программы и системы управления по другим аспектам безопасности авиационной деятельности находятся в стадии разработки. Настоящий стандарт является основой для разработки подробных стандартов по формированию и внедрению систем управления безопасностью в различных предприятиях авиационной отрасли.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Воздушный транспорт

МЕНЕДЖМЕНТ БЕЗОПАСНОСТИ АВИАЦИОННОЙ ДЕЯТЕЛЬНОСТИ В ГРАЖДАНСКОЙ АВИАЦИИ

Основные положения

Air transport. Management of aviation activity in civil aviation. Basic principles

Дата введения — 2017—07—01

1 Область применения

Настоящий стандарт определяет требования к системе менеджмента безопасности авиационной деятельности для организаций авиационной отрасли, когда она:

а) нуждается в демонстрации своей способности постоянно поддерживать уровень безопасности не ниже приемлемого;

б) нацелена на повышение безопасности авиационной деятельности посредством результативного применения системы.

Объектом стандартизации являются основные положения, определяющие содержание процесса разработки, внедрения и функционирования системы менеджмента безопасности авиационной деятельности (СМБАД) на уровне поставщика авиационного обслуживания как совокупности систем управления безопасностью полетов, авиационной безопасностью, экологической, производственной и информационной безопасностью

Цель настоящего стандарта — обеспечить единый подход разработчиков к нормотворчеству в области менеджмента безопасности авиационной деятельности для обеспечения интеграции разрабатываемых отраслевых норм и правил в единую систему управления безопасностью Авиационного Комплекса Российской Федерации.

Требования настоящего стандарта являются общими и предназначены для применения всеми организациями авиационной отрасли независимо от их юридической формы, типа, размера и вида деятельности.

2 Нормативные ссылки

В настоящем стандарте использована нормативная ссылка на следующий стандарт:

ГОСТ Р ИСО/МЭК 31010—2011 Менеджмент риска. Методы оценки риска

Примечание — При пользовании настоящим стандартом целесообразно проверить действие ссылочных стандартов в информационной системе общего пользования на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет или по ежегодному информационному указателю «Национальные стандарты», который опубликован по состоянию на 1 января текущего года, и по выпускам ежемесячного информационного указателя «Национальные стандарты» за текущий год. Если заменен ссылочный стандарт, на который дана недатированная ссылка, то рекомендуется использовать действующую версию этого стандарта с учетом всех внесенных в данную версию изменений. Если заменен ссылочный стандарт, на который дана датированная ссылка, то рекомендуется использовать версию этого стандарта с указанным выше годом утверждения (принятия). Если после утверждения настоящего стандарта в ссылочный стандарт, на который дана датированная ссылка, внесено изменение, затрагивающее положение, на которое дана ссылка, то это положение рекомендуется применять без учета данного изменения. Если ссылочный стандарт отменен без замены, то положение, в котором дана ссылка на него, рекомендуется применять в части, не затрагивающей эту ссылку.

Издание официальное

3 Сокращения, термины и определения

3.1 Сокращения

АБ — авиационная безопасность
АНВ — акт незаконного вмешательства
АОН — авиация общего назначения
БАД — безопасность авиационной деятельности
ВС — воздушное судно
ГА — гражданская авиация
ГосПБП — Государственная программа по безопасности полетов
ИБ — информационная безопасность
ИКАО — Международная организация гражданской авиации
МБАД — менеджмент безопасности авиационной деятельности
ОВД — обслуживание воздушного движения
ПАП — предотвращение авиационных происшествий
СМБАД — система менеджмента безопасности авиационной деятельности
СУБП — система управления безопасностью полетов
РУБП — Руководство по управлению безопасностью полетов
УЗ — уровень значимости (информации)
ФАП — Федеральные авиационные правила
SARPs — Standards and Recommended Practices — Стандарты и Рекомендуемая практика

3.2 Термины и определения

3.2.1 **авиационная деятельность** (aviation activity): Организационная, производственная, научная и иная деятельность физических и юридических лиц, направленная на поддержку и развитие авиации, удовлетворение нужд экономики и населения в воздушных перевозках, авиационных работах и услугах, в том числе на создание и использование аэродромной сети и аэропортов, и решение других задач [10].

3.2.2 **авиационная безопасность** (aviation security): Состояние защищенности авиации от незаконного вмешательства в деятельность в области авиации [8].

3.2.3 **акт незаконного вмешательства** (act of unlawful interference): Противоправное действие, в том числе террористический акт, угрожающее безопасной деятельности транспортного комплекса, повлекшее за собой причинение вреда жизни и здоровью людей, материальный ущерб либо создавшее угрозу наступления таких последствий [13].

3.2.4

база данных СМБАД (safety management data base): Совокупность структурированных и взаимосвязанных данных и методов, числовых значений показателей и объектов, относящихся к задаче менеджмента безопасности авиационной деятельности, обеспечивающих добавление, изменение, выборку, обработку и отображение данных с использованием ЭВМ.
[ГОСТ Р 55859—2013]

3.2.5 **безопасность авиационной деятельности** (safety of aviation activity): Состояние, при котором риски, связанные со всеми аспектами авиационной деятельности, снижены до приемлемого уровня и контролируются.

3.2.6 **безопасность полетов** (safety): Состояние, при котором риски, связанные с авиационной деятельностью, относящейся к эксплуатации воздушных судов или непосредственно обеспечивающей такую эксплуатацию, снижены до приемлемого уровня и контролируются [6].

3.2.7

вероятность (probability): Возможность того, что что-то произойдет.
[ГОСТ Р 51897—2011]

3.2.8 **государственная программа по безопасности полетов** (state safety program): Единый комплекс правил и видов деятельности, нацеленных на повышение безопасности полетов [6].

3.2.9 **государственная система управления безопасностью полетов** (state safety management system): Совокупность осуществляемых на государственном уровне мероприятий по выявлению потенциальных и фактических факторов опасности, по оценке риска их проявления, по разработке и принятию

корректирующих действий, необходимых для поддержания приемлемого уровня безопасности полетов, по оценке эффективности мер по управлению безопасностью полетов гражданских воздушных судов [9].

3.2.10

допустимый риск (acceptable risk): Риск, который в данной ситуации считают приемлемым при существующих общественных ценностях.

[ГОСТ Р 51898—2002]

3.2.11 **информационная безопасность** (information security): Защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений и поддерживающей инфраструктуры [7].

3.2.12 **защита информации** (protection of information): Комплекс мероприятий, направленных на обеспечение информационной безопасности [7].

3.2.13 **культура безопасности** (safety culture): Квалификационная и психологическая подготовленность всех лиц, при которой обеспечение безопасности авиационной деятельности является приоритетной целью и внутренней потребностью, приводящей к осознанию личной ответственности и к самоконтролю при выполнении всех работ, влияющих на безопасность.

3.2.14 **менеджмент безопасности авиационной деятельности** (safety management of aviation activity): Скоординированные действия по руководству и управлению безопасностью авиационной деятельности и реализуемые государственными органами и поставщиками обслуживания.

3.2.15 **остаточный риск** (residual risk): Риск, оставшийся после реализации мер воздействия на риск.

3.2.16 **отраслевые нормы и правила** (industry codes of practice): Инструктивный материал, разработанный отраслевым органом для конкретного сектора авиационной отрасли по соблюдению требований Стандартов и Рекомендуемой практики Международной организации гражданской авиации, других авиационных требований к безопасности полетов и считающейся целесообразной передовой практикой [6].

3.2.17 **показатель безопасности полетов** (safety performance indicator): Основанный на данных параметр, используемый для мониторинга и оценки безопасности полетов.

3.2.18

поставщики обслуживания (service provider): Любая организация, предоставляющая авиационное обслуживание, подверженная факторам опасности и рискам во время предоставления своих услуг.

[ГОСТ Р 55588—2013]

3.2.19

последствие (severity of the consequences): Исход события, влияющий на цели.

[ГОСТ Р 51897—2011]

3.2.20 **предотвращение авиационного происшествия** (aviation accident prevention): Целенаправленная деятельность организаций и должностных лиц по выявлению, оценке отклонений и устранению или уменьшению их опасности в работе элементов авиационной системы [11].

3.2.21 **риск безопасности полетов** (safety risk): Предполагаемая вероятность и серьезность последствий или результатов опасности [6].

3.2.22

риск-менеджмент (risk management): Скоординированные действия по руководству и управлению организацией в области риска.

[ГОСТ Р 51897—2011]

3.2.23 **система управления безопасностью полетов** (safety management system): Системный подход к управлению безопасностью полетов, включая необходимую организационную структуру, иерархию ответственности, руководящие принципы и процедуры [6].

3.2.24 **фактор опасности** (hazard): Состояние, предмет или деятельность, обладающие потенциальной возможностью нанести травмы персоналу, причинить ущерб оборудованию или конструкциям, вызвать уничтожение материалов или понизить способность осуществлять предписанную функцию [1].

3.2.25 **целевой уровень безопасности полетов** (safety performance target): Планируемая или предполагаемая целевая установка для показателя(ей) безопасности полетов на заданный период.

3.2.26 **экологическая безопасность** (environment safety): Состояние защищенности природной среды и жизненно важных интересов человека от возможного негативного воздействия хозяйственной и иной деятельности, чрезвычайных ситуаций природного и техногенного характера, их последствий [12].

3.2.27 **уровень безопасности полетов** (safety performance): Достигнутый государством или поставщиком обслуживания уровень безопасности полетов, определяемый установленными ими целевыми уровнями безопасности полетов и показателями безопасности полетов [6].

4 Общая характеристика менеджмента безопасности авиационной деятельности с учетом контекста организации

4.1 Компоненты менеджмента безопасности организации – поставщика обслуживания

4.1.1 МБАД представляет собой скоординированные действия по руководству и управлению организацией — поставщиком авиационного обслуживания, направленные на управление безопасностью авиационной деятельности.

4.1.2 МБАД охватывает все аспекты безопасности, непосредственно относящиеся к АД. Структурная схема системы МБАД, состоящей из пяти подсистем, соответствующих основным аспектам безопасности, приведена на рисунке 1.

4.1.3 Управление по каждому аспекту безопасности имеет особенности, однако единой основой управления является системный подход, включающий построение необходимой организационной структуры, установление иерархии ответственности и внедрение руководящих принципов и процедур.

4.1.4 В каждой из подсистем СМБАД осуществляется:

- обеспечение выполнения нормативных требований безопасности;
- риск-менеджмент, включающий выявление факторов опасности, оценку обусловленных ими рисков и разработку, при необходимости, корректирующих/предупреждающих мероприятий по снижению рисков.

Рисунок 1 — Структура СМБАД

4.2 Область действия системы менеджмента безопасности авиационной деятельности

4.2.1 Организация поставщика обслуживания должна определить границы и применимость системы менеджмента безопасности авиационной деятельности для установления области ее действия. При определении области действия системы менеджмента безопасности авиационной деятельности организация должна учитывать:

- требования соответствующих заинтересованных сторон,
- деятельность организации;
- нормативные требования безопасности по направлениям деятельности;
- условия, в которых организация осуществляет деятельность.

4.2.2 Область действия системы менеджмента безопасности авиационной деятельности должна быть определена и задокументирована и доступна персоналу организации.

5 Требования к системе менеджмента безопасности авиационной деятельности

5.1 Общие требования

5.1.1 Организация должна установить, внедрить, поддерживать в рабочем состоянии и постоянно улучшать систему менеджмента безопасности авиационной деятельности, включая необходимые процессы и их взаимодействия, в соответствии с требованиями настоящего стандарта.

5.1.2 Управлением каждым аспектом безопасности должно осуществляться в соответствии с требованиями нормативных документов, регулирующих данный аспект безопасности.

5.1.3 В систему управления безопасностью каждого аспекта безопасности должны быть включены следующие элементы.

5.1.3.1 Политика безопасности, которая должна:

- содержать обязанности организации в области безопасности, цели управления безопасностью, заявление о выделении всех необходимых ресурсов, описание неприемлемого поведения персонала и обстоятельства, при которых не будут приниматься дисциплинарные меры;
- подписываться ответственным руководителем организации;
- доводиться до сведения всего персонала, размещаться в общедоступных местах и периодически актуализироваться.

5.1.3.2 Цели управления безопасностью, которые должны быть измеримыми, достижимыми, ограниченными во времени; доводиться до персонала организации; периодически пересматриваться.

5.1.3.3 Задачи и функции системы управления безопасностью.

5.1.3.4 Описание обязанностей и ответственности руководства и персонала за управление безопасностью и достижение поставленных целей.

5.1.3.5 Организационную структуру, необходимую для функционирования системы управления безопасностью и достижения поставленных целей.

5.1.3.6 Планирование мероприятий на случай чрезвычайной обстановки, включая описание действий должностных лиц в случае возникновения нештатной ситуации, угрожающей безопасности.

5.1.3.7 Систему риск-менеджмента безопасности.

5.1.3.8 Методы мониторинга, измерения, при необходимости, а также оценка процессов и, при необходимости, изменения процессов, для гарантии достижения желаемых результатов.

5.1.3.9 Возможности для улучшения процессов и системы менеджмента безопасности.

5.1.3.10 Методы обеспечения безопасности, специфичные для каждого аспекта безопасности.

5.1.3.11 Показатели эффективности управления каждым аспектом безопасности.

5.1.3.12 Популяризация вопросов безопасности.

5.1.3.13 Подготовка персонала для выполнения его обязанностей по управлению безопасностью.

5.1.4 Все процессы системы управления безопасностью должны быть описаны в документации поставщика обслуживания.

Модель системы менеджмента безопасности авиационной деятельности представлена на рисунке 2 и основывается на цикле PDCA [Plan (планируй), Do (делай), Check (проверяй), Act (действуй)].

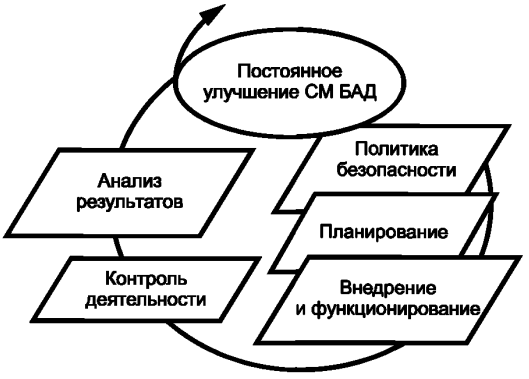

Рисунок 2 — Модель МБАД

5.2 Обязательства и ответственность руководства

5.2.1 Высшее руководство организации — поставщика обслуживания должно гарантировать, что полномочия и ответственность для соответствующих функций установлены, доведены до сотрудников организации и поняты ими.

5.2.2 Высшее руководство должно установить полномочия и ответственность для:

а) обеспечения соответствия системы менеджмента безопасности авиационной деятельности требованиям настоящего стандарта;

б) обеспечения того, что процессы дают ожидаемые результаты;

в) отчетности о функционировании системы менеджмента безопасности, о возможностях улучшения и о необходимости изменений или инноваций, а также для формирования отчетов высшему руководству;

г) повышения безопасности по всей организации;

д) обеспечения целостности системы менеджмента безопасности при планировании и осуществлении изменений в ней.

5.2.3 Высшее руководство должно обеспечить:

- подготовку авиационного персонала;
- предоставление всех ресурсов, необходимых для решения задачи в области безопасности.

5.3 Политика в области безопасности авиационной деятельности

5.3.1 Поставщик обслуживания определяет свою политику в области обеспечения безопасности авиационной деятельности в соответствии с международными и национальными требованиями.

5.3.2 Политика в области обеспечения безопасности авиационной деятельности:

а) отражает обязательство организации по обеспечению безопасности;

б) содержит заявление о предоставлении ресурсов и о подготовке авиационного персонала, необходимых для реализации политики в области безопасности;

в) включает процедуры отчетности в области безопасности;

г) четко указывает, какие виды поведения при осуществлении поставщиком обслуживания авиационной деятельности являются недопустимыми, и обстоятельства, при которых не будут приниматься дисциплинарные меры;

д) подписывается ответственным руководителем организации;

е) размещается в общедоступных местах организации;

ж) периодически пересматривается на предмет сохранения актуальности и соответствия деятельности поставщика обслуживания;

и) доводится до сведения всего персонала.

5.4 Культура безопасности

5.4.1 Действенная культура безопасности в организации является необходимым условием построения действенной СМБАД.

5.4.2 Для эффективного содействия обеспечению безопасности авиационной деятельности руководство обязано:

а) создать такую рабочую среду, в которой все работники осознают свою ответственность за безопасность.

б) поддерживать условия, обеспечивающие ознакомление работников с рисками для безопасности авиационной деятельности, и обеспечить (при необходимости) их достаточными средствами индивидуальной защиты;

в) гарантировать работникам защиту в случае предоставления ими информации о безопасности через систему представления данных.

5.4.3 Система добровольного представления данных о безопасности должна быть конфиденциальной, строиться на принципах ненаказуемости информаторов при отсутствии недопустимого поведения, обеспечивать обратную связь с работниками, информируя их об улучшениях в организации безопасности, сделанных на основании полученных от персонала сообщений.

5.5 Риск-менеджмент безопасности авиационной деятельности

5.5.1 Разработка и внедрение процесса риск-менеджмента

5.5.1.1 Риск-менеджмент является основой системы менеджмента безопасности авиационной деятельности для всех аспектов безопасности.

5.5.1.2 Организация должна разработать, документировать и внедрить процесс риск-менеджмента безопасности, который должен включать следующие процедуры (см. рисунок 3):

- выявление факторов опасности;

- идентификация и оценка риска;
- определение приемлемости риска;
- разработка при необходимости обоснованных мер воздействия на риски;
- оценка уровня остаточного риска;
- внедрение корректирующих мероприятий или отказ от данного вида деятельности;
- мониторинг рисков и оценка эффективности мер воздействия на риски

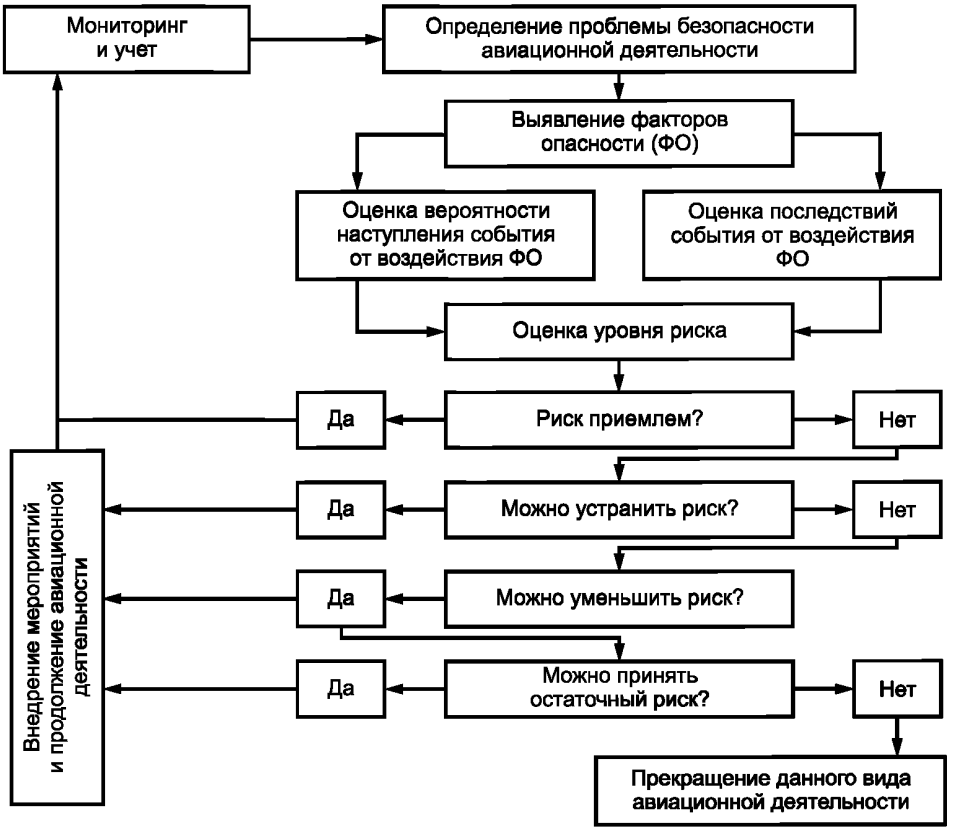

Рисунок 3 — Схема риск-менеджмента безопасности авиационной деятельности

5.5.1.3 Для выявления факторов опасности должны применяться реагирующий, проактивный и прогностический методы.

Реагирующий метод предусматривает анализ результатов расследования авиационных происшествий, инцидентов, производственных происшествий и других событий с ущербом, имевших место в прошлом.

Проактивный метод основан на активном поиске факторов опасности в существующих процессах на основе информации из следующих источников:

- обязательные доклады, отчеты и экспертизы работников;
- данные средств объективного контроля, включая полетную информацию;
- результаты внутренних и внешних инспекционных проверок и аудитов;
- добровольные сообщения работников.

Прогностический метод предусматривает сбор, обработку и анализ данных с целью прогнозирования возможных негативных результатов или событий, анализ системных процессов, тенденций и влияния меняющейся среды, позволяющий выявлять потенциальные факторы опасности в будущем с учетом планируемых изменений.

5.5.1.4 Подробные рекомендации по выявлению факторов опасности для безопасности полетов содержатся в [1].

5.5.1.5 Организация должна применять инструменты и методы идентификации рисков, которые соответствуют ее целям и возможностям, а также рискам, с которыми она столкнулась. Наиболее распространенным в предприятиях авиационного комплекса методом идентификации рисков является качественный метод «матрицы рисков» или метод последствий и вероятностей, рекомендуемый в [1].

5.5.1.6 В практике авиапредприятий могут использоваться и другие методы, рекомендованные в ГОСТ Р ИСО/МЭК 31010—2011.

5.5.1.7 Организация должна применять инструменты и методы идентификации рисков, которые соответствуют ее целям и возможностям, а также рискам, с которыми она столкнулась. Допустимо применение нескольких методов для рисков, связанных с различными аспектами безопасности.

5.6 Определение критериев и показателей эффективности функционирования СМБАД

5.6.1 Организация должна определить критерии и показатели результативности и эффективности системы менеджмента безопасности авиационной деятельности для дальнейшей оценки системы и принятия решения о проведении мероприятий для улучшения системы.

5.6.2 Организация должна установить цели в области безопасности авиационной деятельности для соответствующих функций, уровней и процессов. Цели в области безопасности авиационной деятельности должны:

а) быть согласованы с политикой в области безопасности авиационной деятельности;

б) быть измеримыми;

в) быть достижимыми;

г) быть ограниченными во времени;

д) учитывать применимые требования;

е) быть значимыми с точки зрения безопасности авиационной деятельности;

ж) отслеживаться с точки зрения выполнения;

и) быть доведены до персонала организации;

к) актуализироваться.

5.6.3 Организация должна сохранять документированную информацию о целях в области безопасности авиационной деятельности.

5.6.4 Планируя достижение целей в области безопасности авиационной деятельности, организация должна определить:

а) что необходимо сделать;

б) какие ресурсы потребуются;

в) кто будет ответственным;

г) когда цели будут достигнуты;

д) как результаты будут оцениваться.

5.6.5 Методики расчета показателей безопасности для безопасности полетов, назначения целевых и пороговых уровней приведены в [1].

5.6.6 Методы расчета показателей по отдельным аспектам безопасности приводятся в соответствующих стандартах данной серии.

5.7 Осуществление изменений

5.7.1 В организации должны быть разработаны процедуры выявления внутренних и внешних изменений, которые потенциально могут оказать влияние на безопасность.

5.7.2 Организация должна принять во внимание:

а) цель изменения, предполагаемые последствия;

б) целостность системы менеджмента безопасности авиационной деятельности;

в) доступность ресурсов;

г) распределение или перераспределение ответственности и полномочий;

д) изменение факторов опасности.

5.7.3 В организации должны разрабатываться и внедряться мероприятия по реагированию на выявленные изменения.

6 Требования к процессам управления аспектами безопасности авиационной деятельности

6.1 Управление безопасностью полетов

6.1.1 Государственные требования к системе управления безопасностью полетов поставщиков обслуживания

6.1.1.1 Управление безопасностью полетов является главным компонентом МБАД.

6.1.1.2 В соответствии с SARPs ИКАО [6] и Воздушным законодательством РФ, государство принимает Государственную программу безопасности полетов (ГосПБП) для управления безопасностью

полетов в целях достижения приемлемого уровня безопасности. Принимаемая государством ГосПБП соответствует масштабам и сложности его авиационной деятельности.

6.1.1.3 Государством устанавливается подлежащий достижению приемлемый уровень безопасности полетов.

6.1.1.4 В рамках ГосПБП государство требует внедрения СУБП следующими, находящимися под его контролем, поставщиками обслуживания:

- учебными организациями, которые подвержены влиянию рисков для безопасности полетов, связанных с выполнением полетов ВС в ходе предоставления ими своих услуг;
- эксплуатантами самолетов или вертолетов, имеющими разрешение на выполнение коммерческих авиаперевозок [2];
- утвержденными организациями по техническому обслуживанию, предоставляющими услуги эксплуатантам самолетов или вертолетов, выполняющими международные коммерческие авиаперевозки;
- организациями, ответственными за конструкцию типа или изготовление ВС [2], [3];
- поставщикам ОВД согласно [4];
- эксплуатантам сертифицированных аэродромов согласно [5].

6.1.1.5 СУБП поставщиков обслуживания подлежат согласованию с государством.

6.1.1.6 СУБП поставщика обслуживания:

- создается в соответствии с элементами концептуальных рамок, приведенных в п. 6.1.2;
- соответствует масштабу деятельности поставщика обслуживания и специфики предоставляемых им авиационных продуктов или услуг.

6.1.1.7 СУБП должна включать:

- процесс выявления факторов опасности и оценки соответствующих рисков;
- процесс разработки и реализации мер для поддержания приемлемого уровня безопасности полетов;
- процесс обеспечения постоянного мониторинга и регулярной оценки эффективности СУБП.

6.1.2 Структура системы управления безопасностью полетов поставщика обслуживания

6.1.2.1 SARPs ИКАО устанавливают следующие концептуальные рамки для СУБП, определяющие ее 4 компонента и 12 элементов:

1) политика и цели обеспечения безопасности полетов;
   а) обязанности и ответственность руководства,
   б) иерархия ответственности за безопасность полетов,
   в) назначение ведущих сотрудников, ответственных за безопасность полетов,
   г) координация планирования мероприятий на случай аварийной обстановки,
   д) документация по СУБП;
2) риск-менеджмент безопасности полетов;
   а) выявление факторов опасности,
   б) оценка и уменьшение рисков безопасности полетов;
3) обеспечение (гарантии выполнения требований) безопасности полетов;
   а) контроль и количественная оценка уровня безопасности полетов,
   б) контроль за изменениями,
   в) постоянное совершенствование СУБП;
4) популяризация вопросов безопасности полетов;
   а) подготовка кадров и обучение,
   б) обмен информацией о безопасности полетов.

6.1.2.2 Каждый поставщик обслуживания разрабатывает РУБП, которое подлежит утверждению в уполномоченном государственном органе гражданской авиации в установленном порядке.

6.1.2.3 Вопросы стандартизации разработки, внедрения и совершенствования СУБП поставщиками авиационного обслуживания, а также вопросы формирования корпоративных баз данных в рамках СУБП приведены в соответствующих стандартах серии «Менеджмент безопасности авиационной деятельности».

6.1.3 Взаимодействие государственной программы безопасности полетов и СУБП поставщиков обслуживания

6.1.3.1 Управление безопасностью полетов реализуется на уровне государства (ГосПБП) и организаций, участвующих в авиационной деятельности (поставщиков авиационного обслуживания).

6.1.3.2 При этом системы управления безопасностью полетов на уровне государства и поставщика обслуживания принципиально отличаются, поскольку регулируемые ими процессы ориентированы на разные цели.

6.1.3.3 Цель государства — обеспечение общественной безопасности, цель поставщика обслуживания — выполнять производственную работу в целях удовлетворения заказчика и получения прибыли. Государство устанавливает требования, осуществляет нормативное регулирование и выполняет надзорные функции.

6.1.3.4 Поставщик обслуживания в условиях рыночной экономики решает, прежде всего, задачу достижения производственных целей путем удовлетворения запросов потребителей.

6.1.3.5 Взаимодействие государственных и корпоративных программ управления безопасностью полетов призвано обеспечить гармоничное и безопасное развитие отрасли.

6.1.4 Управление безопасностью полетов и принципы предотвращения авиационных происшествий

6.1.4.1 ПАП является главной целью управления безопасностью полетов. Основными принципами ПАП являются: системность подхода, непрерывность деятельности и действенность реализации мероприятий.

6.1.4.2 В полной мере СУБП поставщика обслуживания должна реализовывать эти принципы в рамках функционирования действующих систем риск-менеджмента с учетом возросших возможностей по обработке данных. В таких системах используется подход метода ПАП по выявлению факторов опасности на основе общепринятой модели «Человек—Машина—Среда» с учетом схемы развития «организационного происшествия», при котором выделяются следующие объекты анализа:

а) человек:
- профессиональный отбор;
- профессиональная подготовка;
- профессиональная деятельность;
- физическое состояние;
- психофизиологическое состояние;

б) техника:
- проектирование;
- изготовление;
- испытания;
- эксплуатация;
- техническое обслуживание;
- ремонт;

в) окружающая среда:
- состояние среды;
- внешние воздействия;

г) организация:
- планирование;
- управление;
- контроль и учет.

6.1.4.3 В системе риск-менеджмента каждого компонента БАД (4.1) указанный подход реализуется с учетом специфических особенностей аспекта безопасности. Конкретные методы и принципы реализации рассматриваются в соответствующих стандартах СМБАД.

6.2 Требования к управлению авиационной безопасностью

6.2.1 Обеспечение авиационной безопасности гражданской авиации осуществляется в соответствии с законодательством Российской Федерации и включает мероприятия, направленные на предупреждение и пресечение актов незаконного вмешательства в деятельность гражданской авиации.

6.2.2 Главный оператор (оператор), имеющий в своем составе службу АБ, является организацией — юридическим лицом с особыми уставными задачами согласно законодательству РФ.

6.2.3 Структура, штаты и конкретные функции службы АБ аэропорта устанавливаются исходя из объемов работы и особенностей режима работы аэропорта в соответствии с федеральными законами, ВК РФ, федеральными авиационными правилами и иными нормативными правовыми актами по вопросам АБ.

6.2.4 Службы АБ аэропортов и службы АБ эксплуатантов, аэропортовых организаций, а также уполномоченные главным оператором (оператором) специализированные организации по предоставлению услуг в области АБ являются службами (организациями) с особыми уставными задачами.

6.2.5 Службы АБ аэропортов и службы АБ эксплуатантов (авиационных предприятий) оснащаются служебным оружием и специальными средствами в соответствии с законодательством Российской Федерации.

6.2.6 АБ обеспечивается посредством:

- предотвращения доступа посторонних лиц и транспортных средств в контролируемую зону аэродрома и (или) аэропорта;

- охраны воздушных судов на стоянках в целях исключения возможности проникновения на воздушные суда посторонних лиц;

- исключения возможности незаконного провоза на воздушном судне оружия, боеприпасов, взрывчатых, радиоактивных, отравляющих, легковоспламеняющихся веществ и других опасных предметов и веществ, а также введения особых мер предосторожности при разрешении их провоза;

- реализации мер противодействия актам незаконного вмешательства в деятельность гражданской авиации и иных мер, в том числе мер, осуществляемых с участием правоохранительных органов;

- предполетного и послеполетного досмотров.

6.2.7 Главный оператор аэропорта разрабатывает и осуществляет программу обеспечения АБ аэропорта посредством применения правил, практики и процедур, учитывающих аспекты безопасности, регулярность полетов, а также координирует деятельность служб АБ и подразделений, осуществляющих охрану аэропортов и объектов их инфраструктуры.

6.2.8 Юридические и физические лица, осуществляющие деятельность на территории аэропорта, в пределах своих полномочий осуществляют мероприятия по выполнению программы обеспечения АБ аэропорта.

6.2.9 Каждый аэропорт должен иметь специальные помещения и технические средства для производства досмотра пассажиров, членов экипажей ВС, авиационного персонала, ручной клади, багажа, грузов, почты и бортовых запасов.

6.2.10 Правила производства досмотра, устанавливаются ФАП.

6.2.11 Службы АБ имеют права на задержание граждан, нарушивших требования АБ, для передачи их правоохранительным органам, а также на приостановление отправки багажа, груза и почты, содержащие предметы и вещества, запрещенные к воздушным перевозкам.

6.2.12 В случаях, если жизни и здоровью пассажиров, членов экипажа воздушного судна или других граждан угрожает опасность, применять иные меры в соответствии с законодательством РФ.

6.2.13 Материально-техническое и финансовое обеспечение АБ в аэропортах осуществляется за счет: федерального бюджета, бюджетов субъектов РФ, местных бюджетов, целевых сборов (аэропортовых), предусмотренных в установленном порядке, а также других источников, не противоречащих законодательству РФ.

6.2.14 Требования, предъявляемые к подразделениям (организациям), осуществляющим охрану аэродрома и (или) аэропорта и порядок их выполнения устанавливаются ФАП.

6.2.15 При выполнении международных полетов предполетный досмотр, а также послеполетный и иные виды контроля в случае их проведения, проводятся после осуществления пограничного и таможенного контроля, в соответствии с требованиями, установленными международными договорами РФ, Федеральными законами и ФАП.

6.2.16 Общие требования в области АБ и порядок их выполнения устанавливаются ФАП с учетом международного законодательства и международной практики в указанной области.

6.2.17 В соответствии с законодательством РФ для обеспечения защиты деятельности ГА от актов незаконного вмешательства в случае угрозы или наличия реальной возможности совершения акта незаконного вмешательства в деятельность ГА могут вводиться дополнительные меры авиационной безопасности в РФ, субъектах РФ, отдельных аэропортах и у эксплуатантов.

6.3 Требования к управлению экологической безопасностью авиационной деятельности поставщиков обслуживания

Основными задачами при разработке, внедрении, поддерживании функционирования или улучшении Системы управления экологической безопасностью являются следующие:

- признание факта, что экологический менеджмент является одним из главных приоритетов поставщика обслуживания;

- разработка и поддерживание обмена информацией и конструктивное сотрудничество с внутренними и внешними заинтересованными сторонами;

- идентификация экологических аспектов деятельности, продукции и услуг поставщика обслуживания;

- идентификация законодательных и других требований, относящихся к экологическим аспектам поставщика обслуживания, которые поставщик обслуживания обязался выполнять;

- обеспечение согласия со стороны руководства и всех лиц, работающих для поставщика обслуживания или по его поручению, в отношении охраны окружающей среды, с четким установлением, а также выполнением ими требований отчетности и ответственности;
- поощрение экологического планирования на протяжении всего жизненного цикла продукции или услуг;
- разработка процесса достижения экологических целей и выполнения экологических задач;
- обеспечение необходимыми и достаточными ресурсами, в том числе с целью обучения, для обеспечения соответствия законодательным и другим требованиям, которые поставщик обслуживания обязался выполнять, для достижения экологических целей и выполнения экологических задач на постоянной основе;
- оценка экологической результативности, исходя из экологической политики поставщика обслуживания, целей и задач и, где это применимо, поиск возможности улучшения;
- разработка процесса менеджмента, включая проведение аудита и анализа системы экологического менеджмента, а также идентификация возможности улучшения системы и, соответственно, повышения экологической результативности, а также поощрение подрядчиков и поставщиков при разработке ими собственных систем экологического менеджмента.

6.4 Требования к управлению производственной безопасностью поставщика обслуживания

6.4.1 Управление можно представить как непрерывный процесс последовательно осуществляемых стадий — оценка параметров условий труда, формирование целей и постановка задач, составление программ, оперативное управление программами, оценка эффективности осуществления программ и стимулирование исполнителей.

Алгоритм процесса управления производственной безопасностью представлен следующим образом (рисунок 4).

6.4.2 Система управления производственной безопасностью включает организационную структуру, деятельность по планированию, распределению ответственности, процедуры, процессы и ресурсы для разработки, внедрения, достижения целей, анализа результативности политики и мероприятий охраны труда организации.

6.4.3 Цели управления производственной безопасностью. Одним из важнейших принципов организации производства является создание безопасных и безвредных условий труда на всех стадиях производственного процесса. В связи с этим основной целью управления производственной безопасностью является совершенствование организации работы по обеспечению безопасности, снижению травматизма и аварийности путем решения комплекса задач по созданию безопасных и безвредных условий труда, лечебно-профилактическому и санитарному обслуживанию работников.

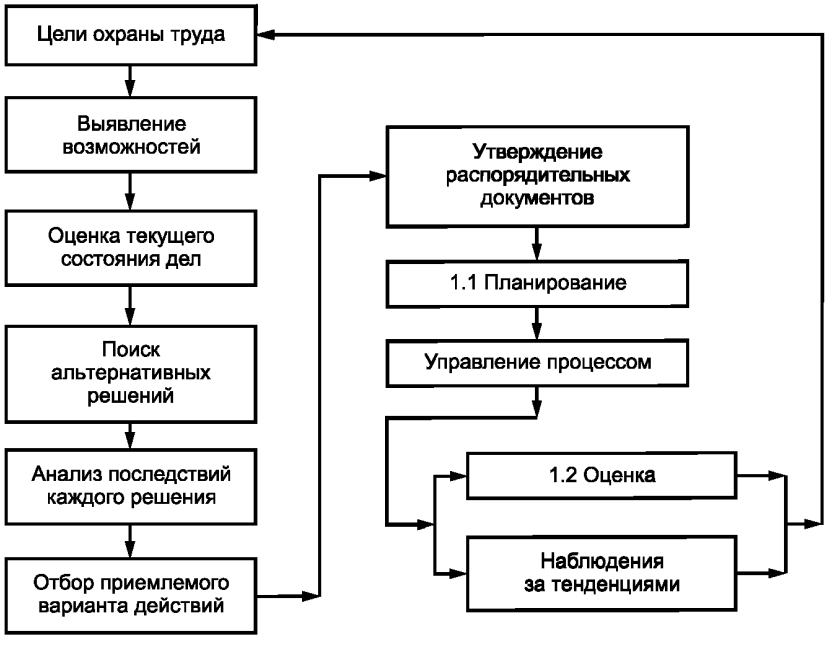

Рисунок 4 — Схема процесса управления производственной безопасностью в организации

6.4.4 Основными задачами, направленными на достижение конечной цели создания безопасных и безвредных условий труда в цехах, на участках и рабочих местах, являются:

- обеспечение безопасности технологических процессов и оборудования;
- обеспечение безопасности зданий и сооружений;
- нормализация санитарно-гигиенических условий;
- обучение работающих и пропаганда правил и норм производственной безопасности;
- организация лечебно-профилактического обслуживания работников;
- обеспечение оптимальных условий труда и отдыха;
- обеспечение работников средствами индивидуальной защиты;
- санитарно-бытовое обслуживание работников;
- профессиональный отбор работников.

6.4.5 К функциям управления производственной безопасностью относятся: функции учета, анализа и оценки, функции контроля, планирования и прогнозирования, стимулирования, организации, координации и регулирования.

6.4.6 Объекты управления производственной безопасностью. В качестве общего управления в Системе управления экологической безопасностью принята деятельность функциональных служб и структурных подразделений по обеспечению безопасных и безвредных условий труда на рабочих местах, производственных участках, в цехах и на предприятии в целом.

6.5 Управление информационной безопасностью

6.5.1 Обеспечение информационной безопасности достигается путем управления совокупностью организационных и технических мер защиты информации, направленных на нейтрализацию угроз безопасности информации, на локализацию и минимизацию последствий от возможной реализации угроз безопасности информации.

6.5.2 Принимаемые организационные и технические меры защиты информации должны обеспечивать доступность информации (исключение неправомерного блокирования информации), ее целостность (исключение неправомерного уничтожения, модифицирования информации), а также, при необходимости, конфиденциальность (исключение неправомерного доступа, копирования, предоставления или распространения информации).

6.5.3 Для обеспечения информационной безопасности назначается структурное подразделение или должностное лицо, ответственные за защиту информации, применяются средства защиты информации, прошедшие оценку соответствия в соответствии с законодательством Российской Федерации о техническом регулировании.

6.5.4 Для обеспечения информационной безопасности поставщик обслуживания должен осуществлять следующие мероприятия:

а) формирование требований к защите информации;

б) разработка системы защиты информации;

в) внедрение системы защиты информации и ввод ее в действие;

г) обеспечение защиты информации в ходе эксплуатации.

6.5.4.1 При формировании требований к защите информации необходимо определить угрозы безопасности информации и разработать на их основе модели угроз безопасности информации.

Модель угроз безопасности информации должна содержать описание возможностей нарушителей (модель нарушителя), способов (сценариев) реализации угроз безопасности информации и последствий от нарушения свойств безопасности информации (доступности, целостности, конфиденциальности).

6.5.4.2 Разработка системы защиты информации включает проектирование системы защиты информации и разработку эксплуатационной документации на систему защиты информации.

При проектировании системы защиты информации определяются типы субъектов доступа (пользователи, процессы и иные субъекты доступа) и объектов доступа, являющихся объектами защиты (телекоммуникационное оборудование, исполнительные устройства, иные объекты доступа), а также определяются методы управления доступом (дискреционный, мандатный, ролевой или иные методы) и типы средств защиты информации, обеспечивающие реализацию технических мер защиты информации.

6.5.4.3 Внедрение системы защиты информации осуществляется в соответствии с проектной документацией на систему защиты информации и включает внедрение организационных мер защиты информации, установку и настройку средств защиты информации и испытания системы защиты информации.

6.5.4.4 Обеспечение защиты информации в ходе эксплуатации осуществляется в соответствии с эксплуатационной документацией на систему защиты информации и включает анализ угроз безопасности информации и рисков от их реализации, менеджментом информационной безопасности и выявлением инцидентов в ходе эксплуатации и реагированием на них.

6.5.5 Организационные и технические меры защиты информации в зависимости от угроз безопасности информации должны обеспечивать:

а) идентификацию и аутентификацию субъектов доступа и объектов доступа;

б) управление доступом субъектов доступа к объектам доступа;

в) регистрацию событий безопасности;

г) антивирусную защиту;

д) обнаружение и предотвращение вторжений;

е) анализ защищенности информации;

ж) информирование и обучение персонала;

и) анализ угроз безопасности информации и рисков от их реализации.

6.5.5.1 Меры по идентификации и аутентификации субъектов доступа и объектов доступа должны обеспечивать присвоение субъектам и объектам доступа уникального признака (идентификатора), сравнение предъявляемого субъектом (объектом) доступа идентификатора с перечнем присвоенных идентификаторов, а также проверку принадлежности субъекту доступа предъявленного им идентификатора (подтверждение подлинности).

6.5.5.2 Меры по управлению доступом субъектов доступа к объектам доступа должны обеспечивать управление правами и привилегиями субъектов доступа, разграничение доступа субъектов доступа к объектам доступа на основе совокупности установленных правил разграничения доступа, а также обеспечивать контроль соблюдения этих правил.

6.5.5.3 Меры по регистрации событий безопасности должны обеспечивать сбор, запись, хранение и защиту информации о событиях безопасности, а также возможность просмотра и анализа информации о таких событиях и реагирование на них.

6.5.5.4 Меры по антивирусной защите должны обеспечивать обнаружение компьютерных программ либо иной компьютерной информации, предназначенной для несанкционированного уничтожения, модификации, копирования информации или нейтрализации средств защиты информации, а также реагирование на обнаружение этих программ и информации.

6.5.5.5 Меры по обнаружению и предотвращению вторжений должны обеспечивать обнаружение действий, направленных на несанкционированный доступ к информации, воздействия на информацию в целях ее уничтожения, искажения и блокирования доступа к информации, а также реагирование на эти действия.

6.5.5.6 Меры по анализу защищенности информации должны обеспечивать контроль уровня защищенности информации путем проведения мероприятий по выявлению и анализу уязвимостей, состава программного обеспечения и технических средств и правильности функционирования средств защиты информации.

6.5.5.7 Меры по информированию и обучению персонала должны обеспечивать информирование персонала об угрозах безопасности информации, о правилах эксплуатации системы защиты информации, а также теоретическое и практическое обучение (в том числе проведение тренировок) по эксплуатации системы защиты информации.

6.5.5.8 Меры по анализу угроз безопасности информации и рисков от их реализации должны обеспечивать периодический анализ изменения угроз безопасности информации, а также периодическую оценку прогнозируемых последствий от реализации угроз безопасности информации.

6.5.6 Для обеспечения информационной безопасности поставщик обслуживания должен осуществлять деятельность в отношении рисков, связанных с информационной безопасностью.

6.5.7 Оценку рисков информационной безопасности определяют в зависимости от уровня значимости информации (УЗ) и вероятности реализации угрозы.

6.5.8 Уровень значимости информации (УЗ) определяется степенью возможного ущерба от нарушения ее целостности (неправомерные уничтожение или модифицирование), доступности (неправомерное блокирование) или конфиденциальности (неправомерные доступ, копирование, предоставление или распространение).

УЗ = [(целостность, степень ущерба) (доступность, степень ущерба) (конфиденциальность, степень ущерба)],

где степень возможного ущерба определяется экспертным или иным методом и может быть:

а) высокой, если в результате нарушения одного из свойств безопасности информации (целостности, доступности, конфиденциальности) возможно возникновение чрезвычайной ситуации федерального или межрегионального характера;

б) средней, если в результате нарушения одного из свойств безопасности информации (целостности, доступности, конфиденциальности) возможно возникновение чрезвычайной ситуации регионального или межмуниципального характера;

в) низкой, если в результате нарушения одного из свойств безопасности информации (целостности, доступности, конфиденциальности) возможно возникновение чрезвычайной ситуации муниципального (локального) характера.

6.5.9 В случае, если для информации не требуется обеспечение одного из свойств безопасности информации (в частности конфиденциальности), уровень значимости определятся для двух других свойств безопасности информации (целостности, доступности). В этом случае:

УЗ = [(целостность, степень ущерба) (доступность, степень ущерба) (конфиденциальность, не применяется)].

6.5.10 Информация имеет высокий уровень значимости (УЗ 1), если хотя бы для одного из свойств безопасности информации (целостности, доступности, конфиденциальности) определена высокая степень ущерба. Информация имеет средний уровень значимости (УЗ 2), если хотя бы для одного из свойств безопасности информации (целостности, доступности, конфиденциальности) определена средняя степень ущерба и нет ни одного свойства, для которого определена высокая степень ущерба. Информация имеет низкий уровень значимости (критичности) (УЗ 3), если для всех свойств безопасности информации (целостности, доступности, конфиденциальности) определены низкие степени ущерба.

6.5.11 Итоговый УЗ устанавливается по наивысшим значениям степени возможного ущерба, определенным для целостности, доступности, конфиденциальности каждого вида информации.

6.5.12 Цели управления информационной безопасностью:

а) СМБАД достигает ожидаемых результатов;

б) предотвратить или снизить риски информационной безопасности;

в) СМБАД постоянно совершенствуется в целом.

Библиография

[1] Руководство по управлению безопасностью полетов (РУБП). Doc. 9859—AN/474, 3-е изд. 2013

[2] Эксплуатация воздушных судов. Приложение 6 к Конвенции о международной гражданской авиации

[3] Летная годность воздушных судов. Приложение 8 к Конвенции о международной гражданской авиации

[4] «Обслуживание воздушного движения. Приложение 11 к Конвенции о международной гражданской авиации

[5] Аэродромы. Приложение 14 к Конвенции о международной гражданской авиации, т. 1 и т. 2

[6] Управление безопасностью полетов. Приложение 19 к Конвенции о международной гражданской авиации

[7] «Об информации, информационных технологиях и о защите информации». Федеральный закон от 27.07.2006 г. № 149-ФЗ

[8] Воздушный кодекс Российской Федерации от 19.03.1997 г. № 60-ФЗ

[9] Постановление Правительства РФ от 18 ноября 2014 г. № 1215 «О порядке разработки и применения систем управления безопасностью полетов воздушных судов, а также сбора и анализа данных о факторах опасности создающих угрозу безопасности полетов гражданских воздушных судов, хранения этих данных и обмена ими»

[10] О государственном регулировании развития авиации ФЗ от 08.01.1997 г. № 10-ФЗ

[11] Методические рекомендации по предотвращению авиационных происшествий, МГА СССР, 1986 г.

[12] Об охране окружающей среды. ФЗ от 10.01.2002 г. № 7-ФЗ

[13] О транспортной безопасности. ФЗ от 09.02.2007 г. № 16-ФЗ

УДК 629.735.083:006.354 ОКС 03.220.50

Ключевые слова: безопасность полетов, авиационная деятельность, риск-менеджмент, менеджмент безопасности

Редактор *М.Н. Штык*
Технический редактор *В.Н. Прусакова*
Корректор *М.И. Першина*
Компьютерная верстка *А.Н. Золотаревой*

Сдано в набор 14.11.2016. Подписано в печать 16.12.2016. Формат 60 × 84 1/8. Гарнитура Ариал.
Усл. печ. л. 2,32. Уч.-изд. л. 2,10. Тираж 27 экз. Зак. 3187.
Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

Издано и отпечатано во ФГУП «СТАНДАРТИНФОРМ», 123995 Москва, Гранатный пер., 4.
www.gostinfo.ru info@gostinfo.ru