EHEST
В составе ESSI

SMS 3

ИНСТРУМЕНТАРИЙ ПО УПРАВЛЕНИЮ БЕЗОПАСНОСТЬЮ ГРУППЫ EHEST

РУКОВОДЯЩИЕ УКАЗАНИЯ

Исполнение для эксплуатантов с простой структурой организации
2-е издание, 2014 г.

European Helicopter Safety Team (Европейская группа по безопасности полетов вертолетов)

Инструментарий по управлению безопасностью

Для эксплуатантов с простой структурой организации

Руководящие указания

Издание 2

Октябрь 2014 г.

О ДОКУМЕНТЕ

Настоящий документ представляет собой руководящие материалы к «Руководству по управлению безопасностью», выпущенному группой EHEST.

«Руководству по управлению безопасностью» EHEST было создано группой специалистов по эксплуатации и системе управления безопасностью Европейской группы по безопасности полетов вертолетов (EHEST). Европейская группа по безопасности полетов вертолетов (EHEST) является европейским отделением Международной группы по безопасности полетов вертолетов (IHST) и вертолетным отделением Европейской стратегической инициативы по безопасности (ESSI).

«Руководство по управлению безопасностью» (SMM) для эксплуатантов с простой структурой организации разработано в октябре 2012 г. с учетом Приложения II правил ЕС по воздушным операциям, главы ORO, подраздел GEN, часть II «Система управления» и соответствующих приемлемых методов установления соответствия (AMC) и руководящих материалов (GM).

Оно будет особенно полезно для эксплуатантов с простой структурой организации, имеющих ограниченный опыт по применению системы управления безопасностью (SMS).

Для предоставления ориентации в определении особенностей и уровня структурной сложности вашей компании ниже представлены критерии, определяющие эксплуатантов со сложной структурой организации, и изложенные в AMC1 ORO.GEN.200(b) «Система управления» следующим образом.

Объем, особенности и структурная сложность деятельности:

(а) Эксплуатант должен рассматриваться как эксплуатант со сложной структурой организации при наличии в его трудовом коллективе более 20 эквивалентов одного сотрудника на полную ставку (FTE), участвующих в деятельности, которая подпадает под действие Регламента (ЕС) № 216/2008 и его правил выполнения.

(б) Эксплуатанты с наличием до 20 эквивалентов одного сотрудника на полную ставку, участвующих в деятельности, которая подпадает под действие Регламента (ЕС) № 216/2008 и его правил выполнения, также могут считаться эксплуатантами со сложной структурой организации на основании оценки следующих факторов:

(1) в отношении структурной сложности — состав и объем работ с привлечением подрядчиков, подлежащих утверждению;

(2) в отношении критериев риска — присутствует ли хотя бы один из перечисленных ниже:

(i) Операции, требующие следующих специальных разрешений: навигация на основе эксплуатационных характеристик (PBN), полет в условиях плохой видимости (LVO), полет на увеличенную дальность на воздушном судне с двумя и более двигателями (ETOPS), подъемные операции на вертолете с применением лебедки (HHO), оказание неотложной медицинской помощи с использованием вертолетов (HEMS), использование системы ночного видения (NVIS) и перевозка опасных грузов (DG).

(ii) Различные типы используемых воздушных судов.

(iii) Окружающая среда (прибрежная зона, горная область и т. д.). «Руководство по управлению безопасностью» (SMM) является главным инструментом для изложения подхода к управлению безопасностью внутри компании. «Руководство по управлению безопасностью» документирует все аспекты управления безопасностью, включая политику в области безопасности, правила техники безопасности и индивидуальные обязанности персонала по обеспечению безопасности.

«Руководство по управлению безопасностью» может быть включено в одно или несколько руководств эксплуатанта. В документе GM1 ORO.GEN.200(a)(5) Система управления — Документация системы управления — Общие положения упоминается следующее:

(а) Не требуется дублировать информацию в других руководствах. Эта информация может содержаться в любом из руководств эксплуатанта (например, руководстве по эксплуатации, руководстве по обучению), которые также могут быть объединены.

(б) Эксплуатант может также по желанию включить некоторую информацию, которая должна быть задокументирована, в отдельные документы (например, процедуры). В этом случае должно быть гарантировано, что руководства содержат правильные ссылки на любые документы, которые хранятся отдельно. Любые такие документы далее должны рассматриваться в качестве неотъемлемой части документации системы управления эксплуатанта.

«Руководство по управлению безопасностью» создано группой профессионалов из состава группы EHEST, обладающих обширным и разнообразным опытом, включая работу в следующих организациях: Европейское агентство по авиационной безопасности (EASA), национальные авиационные администрации, компании-изготовители, эксплуатанты, вертолетные ассоциации, ассоциации эксплуатантов и пилотов и т. д.

Этот образец руководства разработан в помощь эксплуатанту для создания его собственного руководства. Настоящий документ содержит пояснительные примечания и указания, выделенные шрифтом голубого цвета и наклонным.

«Руководство по управлению безопасностью» должно быть адаптировано для надлежащего отражения потребностей эксплуатанта и организации, и не должно применяться просто по принципу «как есть».

Руководство эксплуатанта с простой структурой организации вытекает из более всестороннего «Руководства по управлению безопасностью» для эксплуатантов со сложной структурой организации. См. «Руководство по управлению безопасностью» эксплуатантов со сложной структурой организации для пошагового подхода к организации системы управления безопасностью (SMS).

Пользователь также должен понимать, что наличие совместимого «Руководства по управлению безопасностью» не означает наличие у него готовой к использованию системы управления безопасностью. «Руководство по управлению безопасностью» является исключительно справочным документом, в котором представлено описание и документирование системы управления безопасностью. Далее система управления безопасностью должна создаваться путем соответствующего плана внедрения, для которого требуется ответственный подход со стороны руководства и персонала компании.

План включает оценку организации компании и метод управления безопасностью до внедрения системы управления безопасностью (анализ отличий), создание, внедрение и пересмотр соответствующих процедур и документации, а также обучение по технике безопасности. Он также должен содержать начальную идентификацию факторов опасности и оценку рисков безопасности, с которыми эксплуатант сталкивается при выполнении различных работ.

Для помощи в решении этой задачи в инструментарии по управлению безопасностью группы EHEST приводится пример реестров некоторых типовых факторов опасности и рисков для вертолета, который был разработан отделом безопасности компании Airbus Helicopters. Эти реестры факторов опасности и рисков являются уникальным материалом, который группа EHEST предоставляет всему вертолетному сообществу. Однако необходимо учитывать, что факторы опасности и риски будут различаться в зависимости от эксплуатанта, характера операций и любых существующих на месте препятствий.

ПРИЕМЛЕМЫЕ МЕТОДЫ УСТАНОВЛЕНИЯ СООТВЕТСТВИЯ И РУКОВОДЯЩИЕ МАТЕРИАЛЫ

Переход на сайт, содержащий приемлемые методы установления соответствия (AMC) и руководящие материалы (GM) для главы ORO, указан ниже:
http://easa.europa.eu/system/files/dfu/04%20Part-ORO%20(AMC-GM)_Amdt2-Supplementary%20document%20to%20ED%20Decision%202013-019-R.pdf

Примечание: Наличие отдельной действующей системы управления безопасностью, и которая определена в таком качестве в организационной структуре компании, является единственным путем соблюдения ORO.GEN.200. Другой подход заключается в рассмотрении безопасности в рамках системы управления компанией (комплексный подход). Этот второй подход может стать более подходящим для маленьких и очень маленьких эксплуатантов. Требования ORO.GEN.200 должны соблюдаться независимо от принятого подхода.

Содержание

Глава 1 — Определения

Добавьте любое другое определение, которое вы сочтете полезным, например:

Предохранительный барьер

Контроль риска, направленный на предотвращение нежелательных событий и нежелательных рабочих состояний.

Восстановительный барьер

Контроль риска, направленный на предотвращение таких нежелательных рабочих состояний, которые приводят к аварии или, другими словами, такого сценария происшествия, который перерастает в аварию.

Ослабляющий барьер

Контроль риска, ослабляющий последствия (тяжесть) происшествия или аварии.

Показатель эффективности мер безопасности (SPI)

Параметр безопасности, основанный на данных, который используется для контроля и оценки эффективности мер (ИКАО, документ 9859 AN/474 «Руководство по управлению безопасностью», 3-е издание).

Целевые показатели эффективности мер безопасности (SPO) или плановые показатели эффективности мер безопасности (SPT)

Запланированная или намеченная цель для показателей эффективности мер безопасности на протяжении заданного периода. В настоящем «Руководстве по управлению безопасностью» целевые и плановые показатели рассматриваются в качестве синонимов.

Нежелательное событие (UE)

Событие, ведущее к такой фазе в обострении сценария аварии (нежелательное рабочее состояние), в которой аварии можно избежать только путем проведения успешных мер по восстановлению или случайно.

Нежелательное рабочее состояние (UOS)

Фаза, в которой сценарий аварии уже обострился настолько, что аварии можно избежать только путем проведения успешных мер по восстановлению или случайно.

Глава 2 — Сокращения

Добавьте любое другое сокращение, которое вы сочтете полезным, например:

SPI	Показатель эффективности мер безопасности (SPI)
SPO/SPT	Целевые показатели эффективности мер безопасности (SPO) или плановые показатели эффективности мер безопасности (SPT) (синонимические термины)

Глава 3 — Содержание «Руководства по управлению безопасностью»

См. ORO.GEN.200(a)(5) и связанные приемлемые методы установления соответствия/ «Руководящие указания» (AMCs/GM)

Глава 4 — Политика и цели безопасности

См. ORO.GEN.200(a)(2) и связанные AMCs/GM и AMC1 ORO.GEN.200(a)(1);(2);(3);(5)

Политика безопасности компании должна быть направлена на: совершенствование в направлении высочайших стандартов безопасности, соблюдение всех применимых требований законодательства, соответствие всем применимым стандартам, применение передовой практики и обеспечение подходящими ресурсами.

В политике безопасности должно быть четко заявлено, что целью отчетности и предоставления информации о безопасности и внутренних расследований является повышение безопасности, а не назначение виновных лиц.

Ниже представлен пример политики безопасности, адаптированный из документа ИКАО 9859 AN/474 «Руководство по управлению безопасностью», 3-е издание (ICAO Doc 9859 AN/474 Safety Management Manual, Third Edition):

Политика безопасности

Обеспечение безопасности является одной из ключевых составляющих деятельности компании. Компания привержена принципам развития, внедрения, поддержания и постоянного совершенствования стратегий и процессов для обеспечения реализации всей авиационная деятельности компании в ходе предоставления ее услуг в условиях надлежащего распределения организационных ресурсов, которые направлены на достижение наивысших уровней эффективности мер безопасности и соблюдения требований нормативно-правовых документов.

Ответственность за обеспечение этого наивысшего уровня эффективности мер безопасности несут руководство всех уровней и все сотрудники, начиная с ответственного руководителя [генеральный директор компании (CEO), директор-распорядитель (ED) или управляющий директор (MD), в зависимости от конкретной организации].

Мы подтверждаем свои обязательства:

- Поддерживать управление безопасностью путем предоставления всех необходимых ресурсов, которые приведут к такой корпоративной культуре, которая способствует развитию безопасного выполнения работ, поощряет эффективную отчетность и предоставление информации по безопасности и активно управляет безопасностью с тем же вниманием к результатам, что и внимание к результатам других систем управления в организации.

- Принимать меры для того, чтобы управление безопасностью являлось главной ответственностью всех руководителей и сотрудников.

- Четко определять для всего персонала, руководителей и сотрудников в равной мере их ответственность и обязанности в отношении выполнения мер безопасности в организации и мер системы управления безопасностью в организации.

- Ввести и обеспечить функционирование процессов идентификации факторов опасности и управления рисками, включая систему отчетности и предоставления информации о факторах опасности, для исключения или снижения рисков безопасности последствий наступления факторов опасности, возникающих в результате операций или деятельности, с целью достижения непрерывного улучшения эффективности мер безопасности.

- Гарантировать, что в отношении любого сотрудника, который раскрывает проблемы безопасности посредством системы отчетности и предоставления информации о факторах опасности, не будут предприниматься какие-либо действия, за исключением случаев, в которых такое раскрытие указывает, при отсутствии малейшего основания для сомнения, на грубую небрежность или умышленное или намеренное несоблюдение правил или процедур.

- Соблюдать и всегда, когда это возможно, превосходить требования законодательных и нормативных актов и стандартов.

- Обеспечивать наличие достаточного количества квалифицированных и обученных человеческих ресурсов для реализации стратегий и процессов безопасности.

- Гарантировать, что всему персоналу предоставляется как достоверная и полноценная информация по авиационной безопасности, так и соответствующее обучение, и персонал является компетентным в вопросах безопасности, а ему ставятся только те задачи, которые соответствуют их квалификации.

- Ввести и проводить количественную оценку эффективности мер безопасности в организации в сравнении с реалистичными и целевыми показателями эффективности мер безопасности.

- Непрерывно совершенствовать меры безопасности в организации путем непрерывного контроля и оценки, регулярного обзора и корректировки целей и плановых показателей безопасности, а также старательного приложения усилий для их достижения; а также

- Гарантировать, что поставляемые сторонними поставщиками системы и услуги для поддержки операций организации соответствуют стандартам, которые предъявляются организацией к мерам безопасности.

(Подпись и дата)

Ответственный руководитель

В политике безопасности декларируется, что целью отчетности о безопасности и внутренних расследований является повышение безопасности, а не назначение виновных лиц. С этой целью последний абзац текста политики безопасности должен быть расширен включением отдельного заявления под названием «Защита лиц, предоставляющих информацию: принципы «Just Culture»». Пример представлен ниже:

Защита лиц, предоставляющих информацию: принципы «Just Culture»[1]

Компания обязуется вести деятельность согласно высочайшим стандартам в области безопасности.

Для достижения этой цели необходимо иметь составленные без принуждения и естественные отчеты обо всех авариях, происшествиях, событиях, опасных факторах и рисках и прочих аспектах, которые могут негативно сказаться на безопасном выполнении работ. В связи с этим поощряется ответственное предоставление каждым сотрудником любой информации, касающейся безопасности.

Предоставление информации свободно от предъявления санкций в любых формах. Главной целью предоставления информации является контроль риска и предотвращение аварий и происшествий, а не определение виновных. В отношении любого штатного сотрудника, который раскрывает проблемы безопасности посредством системы отчетности и предоставления информации, какие-либо действия не будут предприниматься, за исключением случаев, когда такое раскрытие указывает, при отсутствии малейшего основания для сомнения, на противозаконное действие, грубую небрежность или умышленное или намеренное несоблюдение правил или процедур.

Применяемый в организации метод сбора, регистрации и распространения информации по безопасности гарантирует в рамках, установленных законом, защиту личных данных для лиц, которые предоставляют информацию о безопасности.

(Подпись и дата)

Ответственный руководитель

[1] Принципы «Just Culture» подразумевают такой уровень культуры, при котором операторы, непосредственно занимающиеся решением проблем, или другие члены персонала не наказываются за их действия, принятые решения или допущенные ошибки, соответствующие их опыту и образованию, но при котором считаются недопустимыми случаи грубой небрежности, умышленных нарушений и деструктивных действий. Принципы «Just Culture» способствуют предоставлению отчетности и информации, поскольку персонал не боится возложения вины за факты, о которых сообщает.

Приемлемое или неприемлемое поведение?

Группа EHEST рекомендует[2] формулировать четкое описание поведения, рассматриваемого компанией как приемлемое (например, совершенно непреднамеренные ошибки) и неприемлемое (например, намеренное несоблюдение процедур, фальсификация документации, саботаж), а также описание его последствий (дисциплинарная политика) таким образом, чтобы разница между двумя этими типами поведения была в полной мере известна и совершенно понятна любому лицу.

Поэтому вопросом первостепенной важности является последовательное применение этого различия таким образом, чтобы решения всегда толковались как справедливые, и персонал не испытывал никакого чувства несправедливости, что могло бы серьезно воспрепятствовать продолжению представления информации о безопасности.

Глава 5 — Ответственность и обязанности по обеспечению безопасности

5.1 Ответственность в области обеспечения безопасности, возлагаемая на ответственного руководителя

См. ORO.GEN.210(a)

Ответственный руководитель имеет полномочия, необходимые для обеспечения финансирования и ведения всей деятельности согласно применимым требованиям.

Ответственным руководителем часто является генеральный директор компании (CEO), директор-распорядитель (ED) или управляющий директор (MD).

Ответственный руководитель несет ответственность за создание и поддержание эффективной системы управления и/или за управление безопасностью в компании.

5.2 Руководитель службы техники безопасности

AMC1 ORO.GEN.200(a)(1);(2);(3);(5) и GM1 ORO.GEN.200(a)(1)

Эксплуатант должен назначить лицо, которое выполняет обязанности руководителя службы техники безопасности.

Руководитель службы техники безопасности несет ответственность за координирование системы управления безопасностью.

Эти функции могут выполняться ответственным руководителем или другим лицом со штатной должностью в компании.

В зависимости от размеров организации эксплуатанта, а также особенностей и уровня структурной сложности его деятельности, руководителю службы техники безопасности в реализации всех задач, относящихся к управлению безопасностью, может помогать дополнительный персонал службы техники безопасности. Укажите, сколько человек из персонала компании назначены в помощь руководителю службы техники безопасности, если это уместно.

Независимо от организационной модели, важно, чтобы руководитель службы техники безопасности оставался единственным контактным лицом в отношении развития, администрирования и обслуживания системы управления безопасностью.

---

[2] Не входит в состав EASA AMC (Приемлемые методы установления соответствия EASA).

Примечание: **Предполагается, что идентификация факторов опасности, оценка риска, оценивание и контроль стали неотъемлемой частью повседневной работы. Повседневный надзор за проведением операций и, следовательно, безопасностью, является обязанностью руководителей и всего персонала. Руководитель службы техники безопасности отвечает за надзор и содействие процессам поддержки других руководителей при разработке процессов, процедур и рабочих правил с целью безопасного выполнения работ персоналом, находящимся под их управлением.**

5.3 Руководитель(-и) (Удалите, если неприменимо)

См. ORO.GEN.210(b)

Термин «руководитель», также используемый в форме «начальник участка деятельности», применяется согласно документу ORO.GEN.210 (b) «Personnel Requirements» (Требования к персоналу), в котором указано, что организацией должно быть назначено лицо или группа лиц, ответственных за обеспечение непрерывного соответствия организации применимым требованиям (правила, стандарты, процедуры компании и т. д.). Это лицо/лица должно подчиняться исключительно ответственному руководителю.

Руководитель(-и) отвечает(-ют) за обеспечение соблюдения всех применимых требований, включая относящиеся к управлению безопасностью.

Примечание: **Руководители являются важной движущей силой эффективного управления безопасностью. Они следят за рассмотрением и должным решением вопросов обеспечения безопасности во всех работах, которыми они управляют.**

5.4 Персонал

См. ORO.GEN.210(c), (d) и (e)

Для упрощения понимания каждым штатным сотрудником своих обязанностей и ответственности в рамках системы управления безопасностью, рекомендуется представить определение обязанностей и ответственности в должностных инструкциях.

5.5 Руководитель службы контроля соблюдения установленных требований (Compliance Monitoring Manager)

См. ORO.GEN.200(a)(6) и связанные AMC и GM

Руководитель службы контроля соблюдения установленных требований отвечает за надлежащее выполнение, поддержание и постоянный пересмотр и улучшение программы контроля соблюдения установленных требований.

Руководитель службы контроля соблюдения установленных требований должен иметь прямой доступ к ответственному руководителю.

Для эксплуатантов с простой структурой организации задачи руководителя службы контроля соблюдения установленных требований может исполнять ответственный руководитель при условии, что он/она обладает необходимой компетентностью. Он или она должны продемонстрировать соответствующие знания, образование и подходящий опыт, относящийся к деятельности компании, включая знания и опыт в контроле соблюдения установленных требований, а также иметь доступ ко всем подразделениям эксплуатанта и, при необходимости, любому оператору-подрядчику.

В том случае, если одно и то же лицо действует в качестве руководителя службы контроля соблюдения установленных требований и руководителя службы техники безопасности, ответственный руководитель в плане своей прямой ответственности за безопасность должен гарантировать, что для обеих функций отведены достаточные ресурсы. Компания должна указать, действует ли руководитель службы контроля соблюдения установленных требований также и в качестве руководителя службы техники безопасности.

Независимость функции контроля соблюдения установленных требований должна быть закреплена гарантией выполнения аудитов и проверок персоналом, который не отвечает за функцию, процедуры и продукты, которые они проверяют.

Глава 6 — Организация и программа контроля соблюдения установленных требований

См. ORO.GEN.200(a)(6) и связанные AMC и GM

Внедрение и применение функции контроля соблюдения установленных требований позволяет эксплуатанту контролировать соответствие всем относящимся к делу требованиям, включая требования системы управления безопасностью. При этом они должны, как минимум и если это целесообразно, контролировать соответствие порядкам действий компании, которые были разработаны для обеспечения безопасной эксплуатационной деятельности.

Программа контроля соблюдения установленных требований охватывает, как минимум и если это целесообразно, диапазон утвержденных операций, руководства, журналы регистрации, записи, стандарты обучения, процедуры и руководства системы управления.

Описание программы контроля соблюдения установленных требований может быть представлено отдельным документом или в другом руководстве.

6.1 Аудиты и проверки

См. GM3 ORO.GEN.200(a)(6)

Документирование аудитов и проверок контроля соблюдения установленных требований может выполняться в «Ведомости контроля соблюдения установленных требований», любых других заключениях, зарегистрированных в «Отчетах о выявленных отклонениях».

См. GM1 ORO.GEN.200(a)(6)(a)

Аудиторы (внутренние или внешние) должны обладать соответствующими знаниями, образованием и опытом, относящимся к деятельности эксплуатанта, включая знания и опыт в контроле соблюдения установленных требований.

Аудитор(-ы) компании демонстрирует дипломатичность, независимость, этику и обладает хорошими навыками коммуникации в устной и письменной формах.

6.2 **Организационная модель** (Удалите, если неприменимо)

Руководителю службы контроля соблюдения установленных требований могут помогать штатный персонал и/или внешняя организация. Опишите организацию контроля соблюдения установленных требований и порядок обеспечения гарантии независимости, планирования аудитов и учета прошлой деятельности и результатов по контролю соблюдения установленных требований.

6.3 Документация по контролю соблюдения установленных требований

В состав этой документации также должны входить программа обучения и программа контроля документации.

Пожалуйста, предоставьте информацию, относящуюся к документацию по контролю соблюдения установленных требований, или укажите ссылку на источник, в котором эта информация зарегистрирована и задокументирована.

6.4 Обучение контролю соблюдения установленных требований

См. AMC1 ORO.GEN.200(a)(6)(e)(1)

Компания должна гарантировать, что весь персонал, привлеченный к управлению функцией контроля соблюдения установленных требований, понимает цели, изложенные в документации системы управления компанией.

См. AMC1 ORO.GEN.200(a)(6)(e)(2)

Компания должна гарантировать, что персонал, отвечающий за управление функцией контроля соблюдения установленных требований, т. е. руководитель службы контроля соблюдения установленных требований и его/ее группа, прошли соответствующее обучение для выполнения этой задачи. Такое обучение должно охватывать требования к контролю соблюдения установленных требований, руководства и процедуры, относящиеся к задаче, методики проведения аудита, ведение отчетности и регистрации.

Пожалуйста, предоставьте информацию, относящуюся к обучению по контролю соблюдения установленных требований, или укажите ссылку на источник, в котором эта информация зарегистрирована и задокументирована.

Глава 7 — Процедура контроля документации

7.1 Общие сведения

См. ORO.GEN.200(a)(5) и связанные AMC и GM

Документация эксплуатанта по системе управления может быть включена в отдельное руководство или одно из руководств согласно требованиям применимых правил выполнения, при этом в необходимых местах должны быть даны перекрестные ссылки. Документация по системе управления компанией должна включать, как минимум, следующую информацию:

- заявление, подписанное ответственным руководителем и подтверждающее, что эксплуатант будет постоянно работать согласно соответствующим требованиям и документации эксплуатанта;
- сфера деятельности эксплуатанта;
- фамилии и функции ответственного руководителя и членов его/ее управленческой группы (см. ORO.GEN.210 (a) и (b));
- схема структуры организации, на которой показаны связи ответственности между лицами, указанными в ORO.GEN.210;
- общее описание и место расположения сооружений и площадок, указанных в ORO.GEN.215;
- процедуры, определяющие подход эксплуатанта к обеспечению соблюдения установленных требований;
- порядок внесения поправок в документацию эксплуатанта по системе управления.

7.2 Контроль и внесение изменений в руководство по управлению безопасностью

«Руководство по управлению безопасностью» должно включать описание порядка его контроля и периодического внесения изменений, а также порядка распространения его редакций в организации.

7.3 Ведение учета

См. ORO.GEN.220(b) и связанные AMC1 и (GM1)

Эффективная система ведения учета гарантирует доступность всех учетных документов при возникновении любой необходимости и в пределах обоснованного времени. Эти учетные документы должны быть систематизированы таким образом, чтобы обеспечивать отслеживаемость и доступность на протяжении всего требуемого периода хранения.

Для обеспечения легкого и быстрого доступа к информации, включая доступ государственных органов, учетные документы компании должны:

- иметь надлежащие ссылочные данные (автор, название, дату выпуска, номер редакции и дату, перечень действующих страниц);
- архивироваться/храниться как учетные документы в течение определенного периода времени; и
- уничтожаться контролируемым методом по прошествии этого установленного периода времени.

Учетная документация должна храниться в бумажной форме, в электронной форме, либо и в том и другом виде. Хранение учетных документов на микропленке или оптических дисках хранения данных также допустимо; однако, независимо от используемой формы, учетные документы должны оставаться удобочитаемыми на протяжении требуемого периода хранения. *Укажите методы хранения, используемые в компании.*

Микрофильмирование или сохранение учетных документов на оптических устройствах хранения данных может выполняться в любое время. Учетные документы должны быть такими же удобочитаемыми, как и оригинальные документы, и оставаться в таком состоянии на протяжении требуемого периода хранения. Период хранения начинается с момента создания или последнего изменения учетного документа.

В системах документации в бумажной форме должны использоваться прочные материалы, которые способны выдержать обычное обращение с документом и его ведение. В системах документации на основе информационных технологий должна быть предусмотрена как минимум одна система резервного копирования, которая должна обновляться в пределах 24 часов с момента любого нового ввода данных. Компьютерные системы должны обладать соответствующей защитой от возможного несанкционированного доступа для предотвращения злонамеренного вмешательства в данные.

Все компьютерные аппаратные средства для резервного копирования данных должны размещаться в месте, отличном от места хранения оригинальных рабочих данных, и в такой среде, которая гарантирует их сохранность в хорошем состоянии. При изменении аппаратных средств или программного обеспечения необходимо уделить особое внимание поддержанию непрерывного доступа ко всем необходимым данным в течение всего периода, указанного в соответствующих правилах выполнения. При отсутствии такого указания все учетные документы должны храниться не менее 5 лет.

Глава 8 — Управление рисками безопасности

См. ORO.GEN.200(a)(3)

Управление рисками безопасности сочетает в себе следующие процессы и компоненты:

- Процессы идентификации факторов опасности, оценки риска и уменьшения последствий воздействия
- Внутреннее исследование безопасности
- Контроль и оценка эффективности мер безопасности
- Управление изменениями
- Непрерывное совершенствование
- План аварийного реагирования (ERP)

Для эксплуатантов с простой структурой организации управление риском безопасности может осуществляться с использованием контрольных перечней факторов опасности либо подобных инструментов или процессов управления рисками, которые интегрированы в деятельность эксплуатанта.

Примечание: Группа EHEST предлагает использовать для оценки и управления рисками безопасности форму оценки, описания, оценивания и контроля риска (RADEC) (см. пример в Приложении 1).

Элементы, влияющие на управление рисками:

ИНФОРМАЦИОННОЕ ВЗАИМОДЕЙСТВИЕ И КОНСУЛЬТИРОВАНИЕ

Хорошее информационное взаимодействие внутри организации и, если уместно, с внешними сторонами (например, заказчиками, партнерами или подрядчиками) должно помочь в обеспечении доступа ко всей необходимой информации и поддержки от всех сторон, на которые может влиять деятельность по управлению риском или предпринимаемые действия. Информационное взаимодействие и консультирование должны происходить на всех важных этапах процесса.

НОРМАТИВНЫЕ ТРЕБОВАНИЯ — РИСКИ, ПРЕДУСМАТРИВАЕМЫЕ НОРМАТИВНЫМИ ТРЕБОВАНИЯМИ

Нормативные требования обычно разрабатываются для контроля общих рисков безопасности, которые возникают из особых или общих факторов опасности, путем применения директивных указаний, технических стандартов в областях технологий, обучения или выполнения задач. Такие факторы опасности, контролируемые нормативными правилами, не должны в дальнейшем рассматриваться в оценках риска, выполняемых эксплуатантом, за исключением наличия доказательства недостаточности регуляторной нормы. Если нормативное правило не является особым, имеет несколько вариантов или прямо предусматривает оценку риска, выполнение оценки факторов опасности является очевидным и требует реализации соответствующих положений.

Примечание по отраслевым стандартам и передовой практике:

Если компания разрабатывает типовые процедуры (SOP) на основе отраслевых стандартов/ передовой практики, она по-прежнему должна выполнять самостоятельную оценку риска, чтобы гарантировать адекватность и адаптацию типовых процедур к своей деятельности.

РЕСУРСЫ ОРГАНИЗАЦИИ

Термин «имеющиеся ресурсы» относится как к возможностям, так и к компетентности:

(i) в отношении самого процесса оценки риска (см. след. страницу); и
(ii) в отношении оцениваемой деятельности (воздушные суда, оборудование, персонал, финансы и т. д.).

При оценке риска обычно рассматриваются текущие ресурсы организации в отношении оборудования и персонала. Одним из выводов по результатам оценки риска может быть то, что эксплуатант не располагает надлежащим оборудованием и персоналом для данной деятельности.

8.1 Содержание управления рисками безопасности

Процесс управления рисками безопасности касается **рисков авиационной безопасности.**

В процессе оценки рисков рассматриваются технические, человеческие, организационные и природные факторы, а также финансовые, юридические или экономические аспекты и все значительные воздействия, которые могут отрицательно влиять на риски авиационной безопасности.

Управление рисками также может распространяться на другие виды рисков, такие как риски в области охраны труда и техники безопасности.

Организация должна обладать способностью идентифицировать все значительные воздействия, которые могут отрицательно повлиять на авиационную безопасность и/или технику безопасности и охрану труда. Однако аспекты техники безопасности и охраны труда не рассматриваются в нормативных правилах ЕС по воздушным перевозкам. Выясните в своем компетентном органе возможные требования к системе управления безопасностью применительно к технике безопасности и охране труда.

8.2 Концепции управления рисками безопасности

Подготовка

ПЛАНИРОВАНИЕ

Оценка риска безопасности инициируется своевременно для обеспечения доступности результатов до наступления необходимости в принятии каких-либо решений относительно рассматриваемой деятельности.

ОПИСАНИЕ СИСТЕМЫ

Описание анализируемой деятельности выполняется в контексте систем и процессов.

РАБОЧАЯ ГРУППА

Руководитель службы техники безопасности определяет необходимость в специальной рабочей группе, в которую входят соответствующие специалисты в предметной области, а также другой персонал, участвующий в работах.

ВЫБОР МЕТОДА И БАЗЫ ДАННЫХ

Для оценки риска могут применяться следующие методы и базы данных:

- Методология, представленная в главе 8 настоящего руководства.
- Руководитель службы техники безопасности принимает решение, использовать ли другие методы и источники, и какие другие методы и источники будут использованы для идентификации факторов опасности и последствий наступления факторов опасности, а также оценки рисков.
- Базы данных компании, которые включают:
  - информацию, полученную по результатам расследования внутренних событий и аварий; и/или

  - o полученные сообщения об отклонениях и предложениях по улучшению; и/или
  - o накопленный опыт в ходе контроля нормальных операций.
- Базы данных компании могут дополняться подобными данными за счет обмена с другими эксплуатантами.
- Руководитель службы техники безопасности примет решение, использовать ли дополнительные источники данных.
- При любой возможности процесс оценки риска будет строиться на опыте, полученном из ранее выполненных оценок рисков.

«Чаша безопасности», описание которой представлено ниже, является хорошей практической моделью риска безопасности и управления риском.

Цель данного подхода заключается в рассмотрении нежелательных событий (UE), представляющих собой промежуточный случай между факторами опасности и рисками и происшествиями и авариями.

Факторы опасности, наступающие по отдельности или в сочетании, могут приводить к наступлению нежелательных событий.

Нежелательные события инициируют фазу в обострении сценария аварии, которая называется нежелательным рабочим состоянием (UOS), в котором развитие сценария дошло до такой точки, что аварии можно избежать только путем проведения успешных мер по восстановлению или случайно.

Меры контроля риска, направленные на предотвращение нежелательных событий и нежелательных рабочих состояний, представляют собой «предохранительные барьеры». Меры контроля, которые предотвращают нежелательное рабочее состояние, приводящее к аварии, обозначаются как «восстановительные барьеры», а меры контроля, которые уменьшают влияние происшествия или аварии, называются «ослабляющими барьерами».

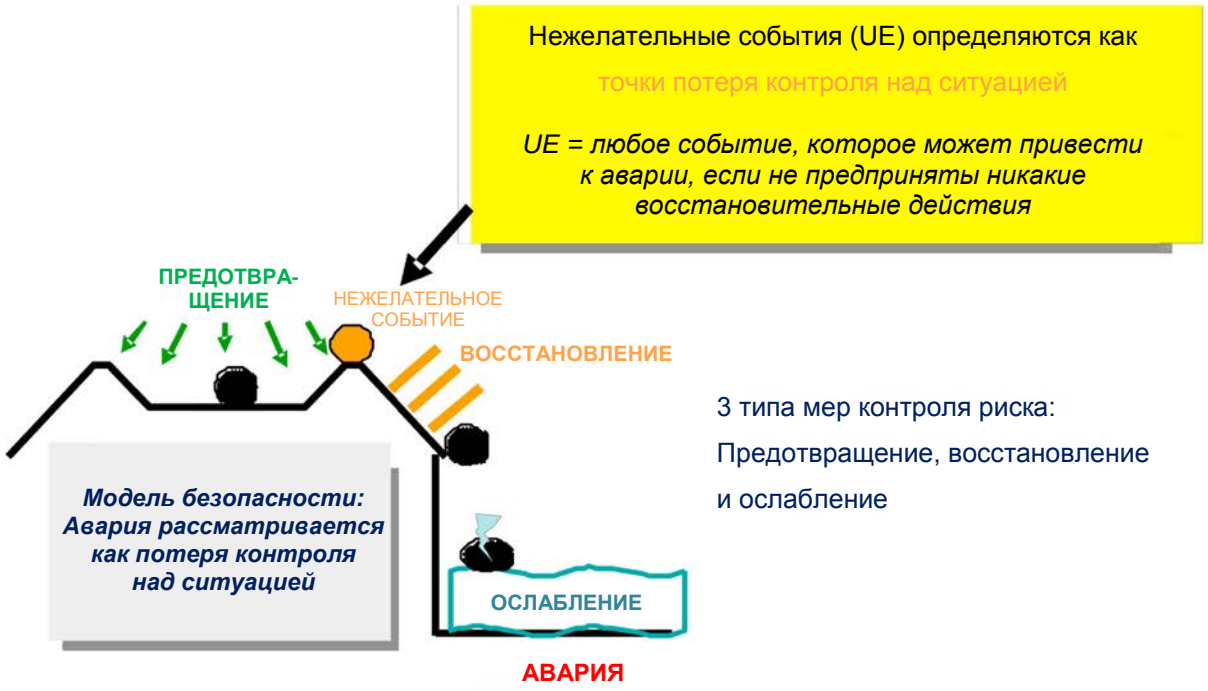

Рис. 1 — Модель контроля рисков безопасности «Чаша безопасности»

(источник: Dédale и Air France)

Модель «чаши безопасности» — интуитивно понятная иллюстрация аварий, рассматриваемых как «потеря контроля» над ситуацией. Чаша представляет собой безопасный контур, в пределах которого должны удерживаться операции, в то время как положение нежелательных событий представляет собой переход к сценариям аварии или происшествия. Восстановление следует за потерей контроля, чтобы предотвратить развитие последствий, и также может восстановить равновесие (возвращение шарика обратно в чашу безопасности). Эта модель также иллюстрирует важность контроля и управления доступными мерами управления риском, и необходимость введения или адаптации мер контроля риска при необходимости.

8.2.1 Идентификация факторов опасности

Хорошей точкой для начала является ответ на следующий вопрос:

Чего я больше всего боюсь в своей работе?[3] Например:

- Столкновение с землей в управляемом полете (CFIT), столкновение с проводами в управляемом полете (CFIW), столкновение с антеннами/проводами, столкновение несущего винта или рулевого винта с препятствиями и т. д.?
- Нестабилизированный заход на посадку?
- Потеря управления, непреднамеренное попадание в сложные метеоусловия?
- Столкновение с землей?
- Столкновение в воздухе?
- Потеря эффекта рулевого винта (LTE)?
- …

Составьте перечень из 10 наиболее рискованных видов работ/ситуаций, которые могут произойти, после чего подробно изучите их.

Факторы опасности — это элементы, которые самостоятельно или в совокупности, могут или могли бы способствовать происшествию или аварии. Они могут быть определены из различных внутренних и внешних источников.

Во время процесса идентификации факторов опасности не следует путать «факторы опасности» с «последствиями наступления факторов опасности». «Факторы опасности» — это ситуации, условия, элементы, окружающая среда, существующие в естественных условиях или часто встречающиеся при работе, которые являются источником опасности, но не обязательно приводят к происшествиям или авариям. Тем не менее, они могут приводить к негативным исходам, которые называются «последствиями наступления фактора опасности».

Рассмотрите следующий пример (источник: компания Airbus Helicopters):

Примеры факторов опасности и их воздействий		
Факторы опасности на рабочем месте	**Пример фактора опасности**	**Пример последствия наступления фактора опасности (причиненный ущерб)**
Инструмент	Нож	Порез

[3] В буклетах по безопасности группы EHEST предлагаются советы и практические рекомендации в отношении того, как рассматривать эти вопросы.

Вещество	Бензол	Лейкемия
Материал	Асбест	Мезотелиома
Источник энергии	Электричество	Удар, смертельное поражение
Состояние	Влажный пол	Скольжение, падение

Процесс идентификации факторов опасности может объединять различные подходы:

Ответный подход (ответная схема) заключается в анализе аварий и происшествий, которые произошли, и попытке понять почему. На основе анализа заявленных аварий и происшествий должны быть поставлены следующие вопросы:

- Какие аварии и происшествия случились с нами и почему?
- По какой причине они произошли? Какие были причинные факторы?
- Какие барьеры или средства контроля рисков не сработали, а какие барьеры оказались успешными? Следует ли укрепить существующие барьеры или ввести новые?

Упреждающий подход (упреждающая схема) заключается в анализе проведения операций для определения потенциальных факторов опасности и оценки и снижения соответствующих рисков до того, как они приведут к аварии или происшествию. Этот подход должен инициировать следующие вопросы:

- Какие аварии и происшествия могли бы случиться с нами и почему?
- По какой причине это могло бы произойти?
- Чувствуем ли мы достаточную защищенность? Существуют ли еще какие-либо действия, которые следует сейчас предпринять для предотвращения наступления аварии или происшествия?

Упреждающая схема также содержит компонент прогнозирования. Он заключается в проведении прогнозного анализа, использующего, например, экстраполяцию данных (в частности, оценку уровня будущего риска на основе данных, собранных за последние 3 или 5 лет) или статистическое моделирование (более сложный путь). Такой прогнозирующий подход направлен на идентификацию и снижение рисков до того, как они станут очевидными (рассмотрение сегодня завтрашнего риска). Этот подход ставит следующие вопросы:

- Какие аварии и происшествия могли бы случиться с нами в будущем и почему?
- Чувствуем ли мы достаточную защищенность? Существуют ли еще какие-либо действия, которые следует сейчас предпринять для предотвращения наступления аварии или происшествия (рассмотрение сегодня завтрашнего риска)?

Прогнозирующий подход и упреждающий подход являются очень эффективными инструментами по управлению безопасностью, они должны основываться на основательных ответных процессах.

8.2.2 Последствия наступления фактора опасности

Факторы опасности отличаются от последствий наступления факторов опасности. Например, кучево-дождевые облака представляют собой фактор опасности[4] для вертолета, летящего поблизости с ними (менее 5 миль). Последствия наступления этого фактора опасности могут включать: сильную турбулентность, которая может вызвать полную потерю воздушного судна; грозовую деятельность, которая может привести к техническому повреждению и/или травмам; град, который может повредить фюзеляж и лопасти; ливневый дождь, который может привести к заглушению двигателя; обледенение, которое увеличивает массу вертолета, влияет на аэродинамический профиль, изменяет профиль лопастей винта и может блокировать кольцо автомата перекоса и т. д.

Последствия могут быть определены на основании информации о факторах опасности и их контексте.

Также, совершенно не имеет значимости заявление, что отсутствие в прошлом происшествий/аварий не означает отсутствие риска! Поэтому важно определять основные факторы опасности и последствия их наступления и оценивать риски, даже если происшествия или аварии не происходят.

8.2.3 Средства контроля рисков

Информацию по средствам контроля рисков можно найти в различных источника, таких как технические публикации, журналы по безопасности, веб-сайты в Интернете, например www.IHST.org, www.EHEST.org, www.skybrary.aero и т. д.

8.3 Этапы управления рисками безопасности

8.3.1 Начальная оценка уровня риска безопасности

Начальный этап заключается в ответе на два следующих вопроса:

- Какова тяжесть последствий наступления факторов опасности, с которыми сталкивается организация?
- Насколько возможны или вероятны эти последствия наступления факторов опасности?

Матрица рисков является хорошим инструментом для описания, оценки и оценивания рисков. В связи с этим EHEST предлагает использовать эту матрицу рисков, описание которой представлено в настоящей главе. Однако, применение матрицы рисков **не является обязательным для эксплуатантов с простой структурой организации**.

8.3.1.1 Анализ возможности или вероятности

Величины возможности или вероятности (насколько возможны или вероятны различные последствия наступления факторов опасности) определяются путем экспертной оценки или на основе периодичности повторения, наблюдавшейся в компании или имеющейся для сектора, типа операции, типа воздушного судна и т. д.

---

[4] И «угрозу» в смысле модели управления опасными факторами и ошибками (TEM). См., например: http://www.skybrary.aero/index.php/Threat_and_Error_Management_(TEM).

Возможность или вероятность может быть выражена с использованием такой терминологии как «очень низкая, низкая, средняя, высокая и очень высокая».

Представленная ниже таблица является примером, которую компания может использовать для определения возможности.

ВЕРОЯТНОСТЬ НАСТУПЛЕНИЯ РИСКА	ОПИСАНИЕ	ЗНАЧЕНИЕ
ЧАСТО	**Вероятно неоднократное возникновение.** Уже происходило в компании (частота > 3 раза в год — ориентировочно*). Часто происходило в истории авиационной отрасли.	**5**
РЕДКО	**Вероятно возникновение время от времени.** Уже происходило в компании (частота < 3 раза в год — ориентировочно*). Происходило в истории авиационной отрасли нечасто.	**4**
МАЛОВЕРОЯТНО	**Возникновение маловероятно, но возможно.** Уже происходило в компании хотя бы раз; или происходило в истории авиационной отрасли редко.	**3**
ПРАКТИЧЕСКИ НЕВЕРОЯТНО	**Возникновение очень маловероятно.** Случаи наступления события в компании неизвестны, но хотя бы один раз уже происходили в истории авиационной отрасли.	**2**
В ВЫСШЕЙ СТЕПЕНИ НЕВЕРОЯТНО	**Возникновение события практически невероятно.** Не происходило в истории авиационной отрасли.[5]	**1**

* Ориентировочно: зависит от размера компании и масштабов деятельности. Используйте показатели, применимые к вашей компании.

Ниже представлены примеры методов,[6] которые компания может применять для причинно-вероятностного анализа **(не является обязательным для эксплуатантов с простой структурой организации):**

- Анализ дерева отказов.
- Анализ характера, последствий и важности отказов (FMECA).
- Диаграммы влияния.
- Диаграммы «галстук-бабочка».
- «Мозговой штурм».

---

5 Отметим, однако, что даже в высшей степени невероятные события могут произойти.

6 Описание этих методов можно найти, к примеру, в интернете на страницах Skybrary или Wikipedia.

На определенной стадии выполнения оценки риска в идентификации новых факторов и барьеров может помочь итеративный процесс. Его результаты затем также могут быть включены в анализ.

Рассмотрение человеческих и организационных факторов и их вероятный вклад в воздействие на сценарий происшествия или аварии может помочь в оценке вероятности последствий наступления фактора опасности. Могут рассматриваться прямые причины («опасные действия»), факторы рабочего места и организационные факторы.

Результаты воздействия существующих средств контроля рисков, которые влияют на цепь событий, также учитываются и документируется с учетом следующих элементов:

- Требования по сертификации.
- Порядок технического обслуживания и ремонта.
- Существующие нормальные и ненормальные процедуры.
- Технические мероприятия/оборудование.
- Обучение.
- Другие человеческие и организационные факторы.

Для установления соответствующих величин возможности или вероятности может выполняться до уровня детали причинный анализ с приложением, например, диаграмм «галстук-бабочка».

8.3.1.2 Анализ степени тяжести

Величины степени тяжести (насколько тяжелыми являются различные последствия наступления фактора опасности) определяются путем экспертной оценки или на основе степеней тяжести, наблюдавшихся в компании или имеющихся для сектора работ, типа операции, типа машин или механизмов и т. д.

Степень тяжести может быть выражена с использованием такой терминологии как «очень маленькая», «маленькая», «средняя», «высокая» и «очень высокая». Значение каждого термина затем выражается словами и/или цифрами или диапазонами.

Ниже представлен пример таблицы, который компания может использовать для определения степени тяжести.

СТЕПЕНЬ ТЯЖЕСТИ НАСТУПЛЕНИЯ СОБЫТИЯ	ОПИСАНИЕ				ЗНАЧЕНИЕ
	ПЕРСОНАЛ	ОКРУЖАЮЩАЯ СРЕДА	МАТЕРИАЛЬНЫЕ ЦЕННОСТИ И АКТИВЫ	РЕПУТАЦИЯ	
КАТАСТРОФИЧЕСКИ ОПАСНО	Несколько смертельных случаев	Масштабные последствия (загрязнение, уничтожение и т. п.)	Катастрофический финансовый ущерб Ущерб более 1 млн евро (*)	Влияние в международном масштабе	**E**
ОПАСНО	Смертельный случай	Трудные для восстановления воздействия	Крупные финансовые убытки с продолжительными последствиями Ущерб менее 1 млн евро (*)	Влияние в национальном масштабе	**D**
СЕРЬЕЗНО	Серьезные травмы	Несущественные локальные воздействия	Значительный финансовый ущерб Ущерб менее 250 тыс. евро (*)	Значительное влияние	**C**
НЕЗНАЧИТЕЛЬНО	Легкие травмы	Небольшое воздействие	Финансовые убытки с небольшими последствиями Ущерб менее 50 тыс. евро (*)	Ограниченное влияние	**B**
ПРЕНЕБРЕЖИМО	Несущественные травмы или отсутствие травм	Пренебрежимые последствия или отсутствие последствий	Финансовые убытки с ничтожными последствиями Ущерб менее 10 тыс. евро (*)	Легкое воздействие или отсутствие воздействия	**A**

* Ориентировочно: зависит от размера компании и масштабов деятельности. Используйте показатели, применимые к вашей компании.

8.3.1.3 Описание и оценивание риска

Описание риска заключается в комбинации возможности или вероятности риска и степени тяжести риска, а оценивание риска заключается в определении приемлемости или допустимости риска (т. е. являются риски приемлемыми или нет).

Описание и оценивание рисков и может выполняться с использованием цветовой матрицы приемлемости рисков.

Пример представлен ниже:

ВЕРОЯТНОСТЬ НАСТУПЛЕНИЯ РИСКА		**СТЕПЕНЬ ТЯЖЕСТИ РИСКА**				
		ПРЕНЕБРЕ-ЖИМО (A)	НЕЗНАЧИ-ТЕЛЬНО (B)	СЕРЬЕЗНО (C)	ОПАСНО (D)	КАТАСТРОФИ-ЧЕСКИ ОПАСНО (E)
ЧАСТО	(5)	**5 A**	**5 B**	**5 C**	**5 D**	**5 E**
РЕДКО	(4)	**4 A**	**4 B**	**4 C**	**4 D**	**4 E**
МАЛОВЕ-РОЯТНО	(3)	**3 A**	**3 B**	**3 C**	**3 D**	**3 E**
ПРАКТИ-ЧЕСКИ НЕВЕРОЯТНО	(2)	**2 A**	**2 B**	**2 C**	**2 D**	**2 E**
В ВЫСШЕЙ СТЕПЕНИ НЕВЕРОЯТНО	(1)	**1 A**	**1 B**	**1 C**	**1 D**	**1 E**

Примечание: **Заполнение матрицы без обоснования подлинной безопасности на основе фактов и взаимосвязи между фактами имеет ограниченное применение. Групповой анализ между специалистами из разных прикладных областей (рабочие группы), относящихся к изучаемой операции (-ям), поможет в оценке риска реалистичным образом. Оценивание рисков должно базироваться на систематическом анализе рассматриваемой операции.**

Неприемлемый уровень риска — **красная** зона в матрице: риск слишком высокий для продолжения операции.

Необходимые действия: Запретить/отложить операцию. Операция может быть возобновлена только после возврата уровня риска на допустимый или приемлемый уровень.

Допустимый уровень риска — **желтая** зона в матрице: уровень риска может быть допустимым для операции при условии реализации соответствующих мероприятий по снижению уровня риска.

Необходимые действия: Выполнить соответствующие мероприятия по снижению уровня риска.

- Для подтверждения оценивания риска: Допущения, сделанные для определения уровня риска и его допустимости, должны быть подтверждены руководителем службы техники безопасности.
- Для разрешения выполнения операций: Руководство, имеющее полномочия на разрешение выполнения операций для этого уровня риска: ответственный руководитель.

Приемлемый уровень риска — **зеленая** зона в матрице: риск допустимый и может быть принят для выполнения операции.

Необходимые действия: Контролировать. Риск рассматривается как контролируемый в достаточной степени и никаких дополнительных мероприятий по снижению уровня риска не требуется. Однако, для дальнейшего снижения риска могут все еще предприниматься действия, если это осуществимо и приемлемо. Кроме того, любые допущения, используемые для выполнения оценки, должны контролироваться для подтверждения того, что они остаются действительными.

Красная, желтая и зеленая зоны также используются в форме RADEC (оценка, описание, оценивание и контроль риска) с такими же толкованиями.

8.3.2 Идентификация дополнительных мер контроля

Идентификация средств контроля рисков

Оценивание риска формирует основу для принятия решения по средствам контроля рисков, называемых также мерами снижения, и для оценки эффективности уже существующих средств контроля риска.

Приоритеты контроля рисков

(Дополнительные) меры контроля риска выбираются на основе следующих приоритетов:

1. Исключение последствий наступления фактора опасности.
2. Снижение возможности или вероятности события.
3. Снижение степени тяжести.

Типы контроля рисков

Примеры контроля рисков включают:

- Пассивный технический контроль (например, система дублирования, противопожарная перегородка).
- Активный технически контроль (например, автоматическая система пожаротушения).

В средствах контроля рисков могут рассматриваться технические, человеческие и организационные факторы, а также факторы внешней среды.

Весь персонал может внести вклад в определение мероприятий по контролю риска, особенно там, где они касаются индивидуального снаряжения (очки, шлемы и другое летное оборудование), через их приемку и использование.

8.3.3 Конечная оценка уровня риска безопасности

Оценка результата контроля рисков

Результаты снижения риска от внедрения новых предусматриваемых средств контроля оцениваются по отношению к:

- Функциональность: Влияет ли мера на способность выполнения работы?
- Выносливость: Будет ли мера эффективной в различных условиях и по прошествии длительного времени?
- Возможным другим результатам, таким как введение новых факторов опасности или новых последствий наступления фактора опасности или перехода рисков («замена рисков»).

Передача риска или замена рисков

При определении мероприятий по контролю рисков должны быть определены любые новые факторы опасности или последствия наступления опасности, которые могут возникать в результате выполнения таких мероприятий.

Риск повторно оценивается с учетом результатов предложенных действий по контролю рисков, что показано в приведенной ниже таблице:

Оцениваемые последствия наступления фактора опасности	**Начальный уровень риска**	**Контроль риска**	**Итоговый уровень риска**
Последствия наступления фактора опасности 1			
Последствия наступления фактора опасности 2			
Последствия наступления фактора опасности n			

Мероприятия не обязательно являются достаточными для того, чтобы вернуть уровень риска обратно на приемлемый или допустимый уровень в первом раунде: если критерии приемлемости риска требуют дальнейшего снижения риска, то сравнение (итеративный процесс) дает описание процесса оптимизации: улучшаются существующие средства контроля риска или рассматриваются новые средства контроля риска, пока риска не будет считаться приемлемым.

Анализ риска должен фокусироваться на безопасности полета. Кроме того, EHEST поощряет рассмотрение безопасности персонала и третьих сторон[7]. Анализ также может быть расширен рассмотрением материала, окружающей среды и репутации компании[8].

Сравнительный анализ затрат и результатов

Альтернативные средства контроля рисков должны подвергнуться сравнительному анализу затрат и результатов[9], который поможет определить наиболее подходящие меры. Снижение риска, которое считается подходящим, должно достичь желаемого повышения безопасности и должно быть экономически обоснованным.

Пример матрицы сравнительного анализа затрат и результатов представлен ниже:

		ВЫГОДА		
		Большая	**Средняя**	**Низкая**
ЗАТРАТЫ	**Низкие**	**1**	**2**	**3**
	Средние	**2**	**3**	**4**
	Большие	**3**	**4**	**5**

Рисунок 2. Матрица простого сравнительного анализа затрат и результатов

Источник: D. Huntzinger, ранее с Airbus Helicopters

Критерии приемлемости в отношении затрат на внедрение средств контроля риска и ожидаемой выгоды должны быть в письменном виде утверждены ответственным руководителем.

Укажите в отдельном документе критерии приемлемости, используемые в вашей компании.

EHEST предлагает использовать единую форму оценки, описания, оценивания и контроля риска (RADEC) для любых случаев, требующих оценки рисков и управления рисками, таких как подготовка типового порядка действий (SOP), управление изменениями и т. д.

Форма RADEC также может поддерживать анализ **отчетов по безопасности.**

Событие можно понимать как реализацию одного или нескольких фактора опасности или последствий наступления фактора опасности:

7 Не правилах ЕС по воздушным операциям. Выясните у своих государственных органов возможные требования к системе управления безопасностью в отношении техники безопасности и охраны труда.

8 Приложение III к правилам ЕС по воздушным операциям, часть ORO.GEN(a) (1);(2);(3);(5) «Система управления» рассматривает только авиационную безопасность.

9 Не входит в состав EASA AMC (Приемлемые методы установления соответствия EASA).

- Перечень факторов опасности (ситуаций), относящихся к событию, указывается в разделе «Фактор опасности» формы RADEC.
- Перечень действительных негативных событий или вероятных негативных событий, относящихся к наступлению фактора опасности, анализируются и приводятся в разделе «Последствия наступления фактора опасности».
- Предложенные дополнительные средства контроля указываются в разделе «Дополнительные средства контроля», где также сообщается статус реализации.

Формы RADEC и связанная с ними документация хранятся в качестве **учетной документации.**

Пример применения формы RADEC представлен в Приложении 1.

8.3.4 Реализация мер контроля рисков

Реализация мер контроля (снижения) риска может требовать составления плана реализации, в котором определяются, в зависимости от характера мероприятий: ответственное лицо, требуемые ресурсы, конечный срок и этапы реализации.

До завершения плана реализации или выпуска его редакции план периодически пересматривается.

8.3.5 Оценивание эффективности контроля риска

Заключительные этапы включают в себя проверку эффективности реализованных мероприятий по контролю риска безопасности. Этот аспект рассматривается в разделе «Контроль и оценка характеристик безопасности» «Руководства по управлению безопасностью» (SMM).

8.4 Предоставление информации о событии и внутренние расследования по безопасности

См. AMC1 ORO.GEN.160 и связанные AMC

Укажите порядок действий, юридический срок и формы, которыми компания сообщает о событиях, серьезных происшествиях и авариях, подлежащих отчетности, вашей государственной авиационной администрации и комитету по расследованию летных происшествий согласно применимым правилам.

В содержание схемы предоставления информации о событии могут также включаться события, о которых полномочные органы не уведомляются.

8.4.1 Схема предоставления информации о событии

См. GM1 ORO.GEN.200(a)(3)

Общей целью схемы предоставления информации о событии является наилучшее использование сообщаемой информации для повышения уровня характеристик безопасности, а не предъявления претензий.

Целями схемы предоставления информации о событии являются:

- Обеспечение возможности выполнения оценки повреждений, значимых для безопасности, для каждого уместного происшествия или аварии, включая предыдущие события подобного характера, с тем, чтобы можно было предпринять любые необходимые действия; и
- Обеспечение распространения информации о соответствующих происшествиях и авариях таким образом, чтобы другие лица и другие эксплуатанты могли сделать выводы из них.

Эта схема является неотъемлемой частью общей функции контроля и дополняет обычные постоянно действующие процедуры и системы «управления», а не предназначена для дублирования или подмены любой из них. Схема является инструментом для определения и анализа тех примеров, в которых процедуры, по-видимому, перестали работать, или применение процедур потерпело неудачу.

Все отчеты о событиях, которые признаны лицом, передающим их, как подлежащие регистрации, будут храниться, поскольку важность таких отчетов может стать очевидной только гораздо позднее.

Каждое событие, идентифицированное с помощью отчетов о событиях, добровольных сообщений или других источников, дает возможность извлечь уроки по безопасности. Обучение на основании опыта возможно только в том случае, если о событиях сообщают и они анализируются, а причины и факторы, вызвавшие их (технические, эксплуатационные, внешней среды), определены и проанализированы.

Ежедневно события (вплоть до простых нарушений функционирования) могут влиять на любой процесс. Некоторые из таких событий определяются как предвестники аварии. Предвестниками аварии считаются такие события, которые без соответствующего уменьшения отрицательных последствий, могут привести к нежелательным событиям или авариям.

Руководитель службы техники безопасности должен регистрировать, анализировать и контролировать эти события.

Форма RADEC поддерживает анализ отчетов по безопасности: события вносятся в формы RADEC для целей анализа, управления риском и учета.

Кроме того, для эксплуатантов со сложной структурой организации в «Руководстве по управлению безопасностью» EHEST приведено несколько **форм и инструментов отчетности о событии**. Вы также можете их рассмотреть, используя файл «Database Incidents.xls» представленный здесь.

О событиях можно сообщать в устной форме, по электронной почте или в письменном виде просто на листе бумаги руководителю службы техники безопасности.

По просьбе информатора с отчетами обращаются как с конфиденциальными и/или анонимными.

Информирование о событиях является важным действием для улучшения безопасности и настоятельно рекомендуется. В ответ компания гарантирует, что информатор(ы) не будут подвергаться наказаниям за сообщения по проблемам безопасности за исключением случая противозаконного действия, грубой небрежности или умышленного или намеренного несоблюдения нормативных правил и применимых процедур. См. раздел «Политика и цели безопасности» в «Руководстве по управлению безопасностью».

8.4.2 Внутренние расследования безопасности (не является обязательным для эксплуатантов с простой структурой организации)

Порядок расследования:

Этап	Пометки
Решение о начале расследования	• Формирование группы расследования.
Планирование деятельности	• Определение и распределение обязанностей. • Определение потребностей расследования.

Сбор данных	• Сбор фактического материала о событии. Могут использоваться следующие уместные источники: o Исследование физических показателей. o Документация и файлы. o Интервью с вовлеченными лицами. o Изучение мероприятий. o Моделирование. o Консультации со специалистами. o База данных безопасности.
Идентификация сценария	• Идентифицировать/реконструировать сценарий.
Анализ сценария	• Проанализировать факты, определить причины и идентифицировать соответствующие факторы опасности. • Объединить все элементы расследования.
Оценка риска	• Определить уровень риска и оценить приемлемость риска.
Контроль риска/анализ уменьшения риска	• Идентифицировать средства контроля риска/снижения риска.
Исправление/ предотвращение	• Определить меры по исправлению/предотвращению.
Предоставление информации по безопасности	• Распространить результаты расследования всем, кого это касается.
Завершение расследования	• Закрыть и архивировать файл.

8.5 Контроль и оценка характеристик безопасности (не является обязательным для эксплуатантов с простой структурой организации)

См. пример формы в Приложении 2.

В случае применения показателей эффективности характеристик безопасности (SPI) и целевых показателей характеристик безопасности (SPO) перечислите их в другом документе, а не в «Руководстве по управлению безопасностью». Также полезно отображение их изменения со течением времени.

Процесс по определению количественных характеристик целевых показателей эффективности безопасности для заданного периода заключается в следующем:

1. Определение базовой линии, относительно которой должна проводиться оценка повышения безопасности.
2. Установление приемлемых, достаточно амбициозных целей и
3. Контроль достижения цели с течением времени и обзор целей при необходимости.

Руководитель службы техники безопасности должен гарантировать, что как целевые показатели характеристик безопасности (SPO), так и показатели эффективности характеристик безопасности (SPI) являются адекватными и документально оформлены.

В ежегодном **обзоре по безопасности** с участием ответственного руководителя будут рассмотрены цели текущего года и поставлены новые для предстоящего года.

ПОЭТАПНЫЙ ПОДХОД К ОЦЕНКЕ ХАРАКТЕРИСТИК БЕЗОПАСНОСТИ **(На усмотрение)**

На различные уровнях развития системы управления безопасностью количество доступных данных по безопасности, вопросов и мероприятий, самых важных для повышения характеристик безопасности, будет разным. Поэтому компания должна принять поэтапный подход к оценке характеристик безопасности[10] на основе трех уровней степени завершенности системы управления безопасностью:

УРОВЕНЬ 1 ВВОДА В ДЕЙСТВИЕ СИСТЕМЫ УПРАВЛЕНИЯ БЕЗОПАСНОСТЬЮ: ИМЕЕТСЯ И ПРИМЕНИМА

На первом уровне система управления безопасностью достигнет согласованности с применимыми требованиями. Показатели эффективности характеристик безопасности (SPI) должны быть сосредоточены на работах, которые требуются для поддержания базового соответствия с нормативными положениями системы управления безопасностью. Они могут быть количественного (численного) или качественного (не численного) характера.

Количественные показатели (примеры):

- число проведенных обзоров по безопасности;
- число штатных сотрудников, прошедших обучение по системе управления безопасностью;
- число проведенных внутренних аудитов в сравнении с плановым показателем;
- и т. д.

Качественные показатели (примеры):

- обратная связь, полученная от штатных сотрудников, в отношении политики безопасности;
- обратная связь, полученная по мероприятиям по безопасности, встречам по безопасности, кампаниям по безопасности, которые компании сумела организовать;
- обратная связь, полученная от штатных сотрудников, в отношении внедренных новых процедур в области внутреннего информирования о событиях или идентификации факторов опасности;
- и т. д.

После того как система управления безопасностью вошла в строй и достигнуто соответствие требованиям, для рассмотрения характеристик безопасности могут быть внедрены показатели нового уровня 2.

УРОВЕНЬ 2 ВВОДА В ДЕЙСТВИЕ СИСТЕМЫ УПРАВЛЕНИЯ БЕЗОПАСНОСТЬЮ: РАБОТАЕТ И ЭФФЕКТИВНА

На этом уровне компания начинает определять более конкретные показатели эффективности безопасности на основе данных по безопасности, которые были собраны в ходе процессов идентификации факторов опасности и внутреннего информирования о событиях (см. соответствующие разделы настоящих «Руководящих указаний»).

Более конкретно, вводятся объективные и надежные показатели «опережения» или «перспективы», такие как:

---

[10] Не входит в состав EASA AMC (Приемлемые методы установления соответствия EASA).

- число оценок рисков, выполненных после организационных изменений;
- процент типовых процедур (SOP), прошедших определение факторов опасности;
- среднее время, потраченное на завершение мероприятий по устранению после проведения внутреннего аудита;
- число внедренных дополнительных процедурных средств контроля;
- и т. д.

На этом уровне развития системы управления безопасностью компания будет получать улучшенную картину по рискам, влияющим на работу, и основательности уже существующих средств контроля риска.

УРОВЕНЬ 3 ВВОДА В ДЕЙСТВИЕ СИСТЕМЫ УПРАВЛЕНИЯ БЕЗОПАСНОСТЬЮ: ПЕРЕДОВАЯ ПРАКТИКА

Уровень 3 является таким уровнем, на котором компания достигла состояния непрерывного накопления знания и совершенствования для всех частей системы управления безопасностью.

На этом уровне развития устанавливаются эффективные процессы идентификации факторов опасности и оценки рисков, которые позволят заимствовать или использовать более совершенный набор показателей эффективности безопасности.

Показатели эффективности характеристик безопасности сосредоточены на рисках, конкретных для компании, которые обнаруживаются работающей системой управления безопасностью с помощью дополнительной информации по безопасности, обнаруженной внутри отрасли или полномочными органами[11].

Показатели эффективности характеристик безопасности (SPI) должны рассматривать уровни рисков и основательность средств контроля рисков.

Мероприятия по снижению рисков фокусируются на тех проблемах, которые представляют самые большие риски или являются проблемами с самым большим потенциалом для улучшения.

Количественные показатели (примеры):

- Число событий с высоким риском (отмечены желтым или красным цветом).
- Среднее значение оценки риска (за период времени, которому соответствуют данные наблюдений, например, 1 год).
- Основательность средств контроля рисков (оценка от 0 до 5, за период времени, которому соответствуют данные наблюдений, например, 1 год).

Также должна быть проведена оценка эффективности любого нового внедренного средства контроля риска.

8.6 Планирование аварийного реагирования

См. AMC1 ORO.GEN,200(a)(1);(2);(3);(5) пункт (f)

Пример плана аварийного реагирования, разработанного EHEST, представлен в отдельном документе

[11] Данные, собранные внутри компании, могут оказаться недостаточными или недостаточно репрезентативными для выполнения реалистичной оценки риска. Поэтому для оценки риска необходимо учитывать соответствующие данные по безопасности в отрасли.

8.7 Управление изменениями

AMC1 ORO.GEN.200(a)(1);(2);(3);(5)

Порядок оценки влияния изменения

1. Установить природу и масштаб изменения(-ий).
2. Определить ключевой персонал, который поможет внедрить изменение и требуемые меры по снижению, а также включить их в процесс управления изменениями.
3. Выполнить начальную оценку влияния, которая будет охватывать:
   - Методики работы компании (руководство по эксплуатации, руководство по стандартизации, экспозиция по организации обучения техническому обслуживанию и ремонту (MTOE) и т. д.).
   - Организацию работы (комплектование персоналом, состав групп, составление графиков, дополнительное обучение и т. п.).
   - Инфраструктуру (перебазирование, место стоянки и т. д.).
   - Техническое обслуживание и ремонт оборудования или воздушного судна.
4. Выполнить анализ риска безопасности (см. раздел «Управление риском»):
   - Идентифицировать факторы опасности, относящиеся к внедрению предложенного изменения и их вероятные последствия.
   - Идентифицировать существующие средства контроля риска и определить, в зависимости от ситуации, дополнительные меры по снижению.
5. Установить план внедрения.
6. Оценить связанные финансовые затраты.
7. Распространить предложенное изменение среди штатного персонала и привлечь его к проекту в попытке заработать хорошую репутацию.
8. Выполнить мероприятия, установленные в плане.
9. Проверить общее воздействие путем создания процесса оценки и контроля характеристик безопасности.

8.8 Постоянное улучшение (не является обязательным для эксплуатантов с простой структурой организации)

Компания будет непрерывно совершенствовать свою систему управления безопасностью[12] и характеристики безопасности.

[12] В приемлемых методах установления соответствия (AMC) только упоминается непрерывное совершенствование характеристик безопасности (результат системы управления безопасностью), но не само совершенствование системы управления безопасностью.

Руководитель службы техники безопасности выполняет обзор системы управления безопасностью (насколько эффективно цели и задачи были выполнены соответственно требованиям) и он/она ежегодно предоставляет ответственному руководителю отчет[13] о системе управления безопасностью (насколько эффективно система работает, этапы внедрения, результаты аудитов и обзоров мероприятий по выполнению, любые вопросы/проблемы и предложения по совершенствованию).

Совершенствование системы управления безопасностью[14]

Непрерывное совершенствование системы управления безопасностью достигается путем:

- Оценки функционирования системы управления безопасностью.
- Идентификации и анализа возможных вопросов/проблем, связанных с применением системы управления безопасностью.
- Внедрения изменений, направленных на совершенствование системы управления безопасностью.
- Контролирования и обзора результатов любых изменений.

Непрерывное совершенствование также может быть достигнуто, когда система управления безопасностью работает уже хорошо.

Меры, которые могут улучшить систему управления безопасностью:

- Упрощенные процедуры.
- Улучшенные обзоры, исследования и аудиты безопасности.
- Улучшенные инструменты отчетности и анализа.
- Улучшенные процессы идентификации факторов опасности и оценки рисков, а также улучшенная информированность в компании о рисках.
- Улучшенные отношения с субподрядчиками, поставщиками и заказчиками в отношении безопасности.
- Улучшенные процессы информационного взаимодействия, включая обратную связь от персонала.

Непрерывное совершенствование системы управления безопасностью может быть нацелено на любой компонент системы управления безопасностью, другими словами, любой предмет, рассматриваемый в данной системе управления безопасностью, имеющий своей целью повышение эффективности системы с течением времени.

Глава 9 — Работы с привлечением подрядчиков

См. ORO.GEN.205 и связанные AMC1 и GM1

Вставьте отдельный документ или таблицу относительно работ компании с привлечением подрядчиков и организаций-подрядчиков.

---

13 Не входит в состав EASA AMC (Приемлемые методы установления соответствия EASA).

14 Не в документах «Порядок реализации» и EASA AMC (Приемлемые методы установления соответствия EASA).

Глава 10 — Распространение знаний по вопросам безопасности

Распространение знаний по вопросам безопасности направлено на распространение культуры безопасности. Весь персонал знакомится с рисками безопасности и понимает, что они являются ключевыми действующими лицами безопасности, и все они вносят вклад в эффективную систему управления безопасностью.

Руководители являются главными действующими лицами в системе управления безопасностью компании. Во всех мероприятиях, которыми они руководят, они демонстрируют приверженность безопасному подходу и заботятся о проблемах обеспечения безопасности. Они подают личный пример и играют важную роль в распространении знаний по вопросам безопасности.

Обучение и эффективные коммуникации по вопросам безопасности — два важных процесса, которые поддерживают распространение знаний в области безопасности.

Глава 11 — Обучение и обмен информацией по безопасности

См. ORO.GEN.200(a)(4) и связанные AMCs/GM

11.1 Обучение

Между обучением и риском безопасности существует связь, поскольку обучение и расширение компетенции представляет собой одно из средств по снижению рисков безопасности. Другие типы средств контроля рисков касаются оборудования или организационных факторов (например, процедур), которые в свою очередь также могут рассматриваться при обучении.

Программа обучения по безопасности может состоять из комбинации самообразования с использованием различных источников обучающих материалов, аудиторного обучения, среды электронного обучения или других типов обучения.

Примечание: **По мере развития системы управления безопасностью и пока не будет предписано иное в порядках реализации, содержание и периодичность обучения должны быть связаны с управлением риском безопасности и оценкой и контролем характеристик безопасности (динамический процесс). Самым высоким рискам, а также тем рискам, для которых контроль особенно зависит от компетентности персонала, должно уделяться больший объем обучающих ресурсов (продолжительнее, чаще и т. п.).**

Представленная ниже таблица является примером обучения по системе управления безопасностью, которую можно проводить для новых членов штатного персонала (вводное обучение) и предусматривать в качестве переподготовки:

Содержание	Цели обучения	Метод/ организатор	Продолжительность/ период действия
Политика безопасности	Понять основные элементы политики безопасности.		
Организация, роли и обязанности	Понять организацию, роли и обязанности применительно к системе управления безопасностью. Каждый должен знать свою роль в системе управления безопасностью.		

Содержание	Цели обучения	Метод/ организатор	Продолжительность/ период действия
Цели безопасности	Понять цели безопасности компании.		
Планирование аварийного реагирования (ERP) (усиленное практическим моделированием)	Понять различные роли и обязанности в плане аварийного реагирования компании. Каждый должен знать свою роль в плане аварийного реагирования.		
Отчеты о происшествиях и авариях	Знать средства и порядок информирования о происшествиях и авариях.		
Процесс управления риском безопасности (SRM), включая роли и обязанности	Понять процесс управления риском безопасности. Каждый должен знать свою роль в процессе управления риском безопасности.		
Непрерывное совершенствование характеристик безопасности	Понять принципы непрерывного совершенствования характеристик безопасности.		
Контроль за установленными требованиями	Понять основные принципы контроля соблюдения установленных требований.		
Ответственность при заключении контрактов на выполнение работ	Понять ответственность компании при заключении контрактов на выполнение работ. Каждый должен знать свою роль и обязанности в применении к этой тематике.		

11.2 Коммуникации

См. ORO.GEN.200(a)(4) и связанные AMCs/GM

Пример средств информирования и информационного взаимодействия представлен ниже:

- Встречи по вопросам безопасности.
- Инструктажи по технике безопасности.
- Электронная почта, обычная почтовая служба, ящики для предложений.
- Информация по безопасности от изготовителей оригинального оборудования, компетентных органов, вертолетных ассоциаций, а также от национальных и международных инициатив по безопасности.
- Кампании по безопасности, плакаты по технике безопасности.
- Информационные бюллетени, журнал компании.
- Сборники по летной безопасности, обзоры публикаций по летным авариям и происшествиям (надлежащим образом обезличенным), произошедшим в компании и за ее пределами.
- Обзорные статьи об исследованиях безопасности, аудиторские отчеты, инспекционные отчеты и обзоры по безопасности.
- Корпоративные форумы или профессиональные социальные сети (например, LinkedIn, Facebook, Twitter и т. д.).
- Подписка на периодические публикации и журналы.

Приложение 1 — Форма оценки, описания, оценивания и контроля риска (RADEC) — ПРИМЕР

ФОРМА ОЦЕНКИ, ОПИСАНИЯ, ОЦЕНИВАНИЯ И КОНТРОЛЯ РИСКА (RADEC)	
Оценка риска №: H001	**Определение:** Приземление на ограниченную площадку
Ссылка: Типовой порядок действий для системы внешней подвески	
Описание операции: Операции с системой внешней подвески в горных областях	
Факторы опасности: Что было или могло бы стать источниками потенциального повреждения, вреда или неблагоприятного воздействия на здоровье в изучаемой окружающей среде? **H 1.** Деревья и растительность **H 2.** Провода, линии электропередач **H 3.** Метеорологические условия **H 4.** Ветер, турбулентность, нисходящие потоки **H 5.** Ограниченные посадочные площадки	
Возможные последствия наступления фактора опасности: Какими были или могли бы быть последствия наступления факторов опасности? **HC 1.** Столкновения несущего винта с наземными препятствиями **HC 2.** Столкновения рулевого винта с наземными препятствиями **HC 3.** Контакт в полете с проводами, линиями электропередач **HC 4.** Травмирование наземного персонала поднимаемым грузом или нисходящим потоком от вертолета **HC 5.** Непреднамеренный или случайный сброс груза **HC 6.** Повреждение на земле **HC 7.** Потеря мощности в полете **HC 8.** Вихревое кольцо **HC 9.** Неконтролируемое раскачивание груза	
Средства контроля, готовые к использованию — Какие средства контроля рисков уже существуют для решения проблемы? **C 1.** Минимальный размер посадочной площадки (25 м x 25 м) **C 2.** Квалификация пилота: не менее 500 л. ч. авиационных работ. **C 3.** До посадки площадка должна быть осмотрена персоналом компании **C 4.** Опознавание на большой и малой высоте перед первой посадкой **C 5.** Порядок действий для системы внешней подвески **C 6.** Указание на карте участков с проводами и линиями электропередач до начала операций с внешней подвеской	
НАЧАЛЬНЫЙ риск безопасности — см. матрицу рисков безопасности (если используете)	
ПРИЕМЛЕМЫЙ	**ДОПУСТИМЫЙ** / **НЕПРИЕМЛЕМЫЙ**

Дополнительные средства контроля — Что еще можно сделать для дальнейшего снижения начальных рисков безопасности до приемлемого уровня?		**Выполнено?**
C 7.	Контакт по радиосвязи наземного персонала с пилотом	ДА
C 8.	Ношение наземным персоналом касок и средств индивидуальной защиты	ДА
C 9.	Минимальная длина троса = длина самого высокого препятствия + 15 футов	ДА
C 10.	Максимальная взлетная масса с грузом понижена на 5%	НЕТ (существующий)

КОНЕЧНЫЙ риск безопасности (см. матрицу рисков безопасности)

~~ПРИЕМЛЕМЫЙ~~	**ДОПУСТИМЫЙ**	**НЕПРИЕМЛЕМЫЙ**

Является ли остаточный риск приемлемым: ☒ ~~ДА~~ НЕТ (если НЕТ, вернитесь к предыдущей секции)

ОЦЕНКА РИСКА ЗАВЕРШЕНА ☒

Приложение 2 — Показатели эффективности характеристик безопасности и цели
(не является обязательным для эксплуатантов с простой структурой организации)

	Пункт	Цели	Характеристик в 20XX г.											
			1	2	3	4	5	6	7	8	9	10	11	12
			Кв. 1			Кв. 2			Кв. 3			Кв. 4		
			1-е полугодие						2-е полугодие					