IMAS 07.14

Первое издание
Февраль 2019 г.

Управление рисками в противоминной деятельности

Директор
службы Организации Объединенных Наций по вопросам противоминной деятельности (UNMAS)
1 United Nations Plaza, 6th Floor
New York, NY 10017
USA (США)

Электронная почта: mineaction@un.org
Телефон: +1 (212) 963 0691
Факс: +1 (212) 963 2498
Веб-сайт: www.mineactionstandards.org

Предупреждение

Настоящий документ является действующим с даты его актуализации, указанной на титульном листе. Так как серия Международных стандартов противоминной деятельности (IMAS) подвергается регулярному пересмотру и редактированию, пользователям следует сверяться с данными о статусе каждого документа на веб-сайте проекта IMAS по адресу http://www.mineactionstandards.org/ или на веб-сайте службы UNMAS по адресу http://www.mineaction.org.

Уведомление об авторских правах

Директор
службы Организации Объединенных Наций по вопросам противоминной деятельности (UNMAS)
1 United Nations Plaza, 6th Floor
New York, NY 10017
USA (США)

Электронная почта: mineaction@un.org

Телефон: +1 (212) 963 0691
Факс: +1 (212) 963 2498

Содержание

Предисловие

Международные стандарты для реализации программ в области гуманитарного разминирования были впервые предложены рабочими группами на международной технической конференции, состоявшейся в Дании в июле 1996 года. Были предписаны критерии для всех аспектов процесса разминирования; рекомендованы стандарты и согласовано новое универсальное определение термина clearance (очистка). В конце 1996 года эти принципы, предложенные в Дании, получили развитие по результатам деятельности рабочей группы под эгидой ООН, и на их основе были разработаны Международные стандарты проведения операций в области гуманитарной очистки от мин. Первое издание было опубликовано службой ООН по вопросам противоминной деятельности (UNMAS) в марте 1997 года.

Содержание этих исходных стандартов было расширено, с тем чтобы включить другие компоненты противоминной деятельности и отразить изменения, внесенные в рабочие процедуры, практические методы и регламенты. Эти стандарты были переработаны и переименованы в Международные стандарты противоминной деятельности (IMAS). Их первое издание было выпущено в октябре 2001 года.

На Организацию Объединенных Наций возлагается общая ответственность за создание условий и стимулов для эффективного управления программами в области противоминной деятельности, включая разработку и сопровождение стандартов. В связи с этим UNMAS является подразделением Организации Объединенных Наций, отвечающим за разработку и сопровождение IMAS. Стандарты IMAS подготавливаются при содействии Женевского международного центра гуманитарного разминирования (GICHD).

Работу по подготовке, пересмотру и редактированию этих стандартов ведут технические комитеты при поддержке со стороны международных, государственных и негосударственных организаций. С последней версией каждого из стандартов, а также с информацией о работе технических комитетов можно ознакомиться по адресу http://www.mineactionstandards.org/. Отдельные стандарты IMAS пересматриваются не реже одного раза в три года, чтобы отразить изменения, происходящие в нормативных документах и практических процедурах противоминной деятельности, а также для того, чтобы внести эти изменения в международные регламенты и требования.

Введение

Управление рисками носит фундаментальный характер по отношению к каждому из аспектов противоминной деятельности. Данный факт проявляется не только в безопасности работы персонала и в обеспечении безопасности конечных пользователей высвобождаемых земель, но и в каждом решении, принимаемом руководителями противоминной деятельности и другими работниками: какие проекты и программы поддерживать, кого нанимать на работу, как вести профессиональную подготовку персонала, какое оборудование приобретать, как поддерживать отношения с ключевыми участниками, каким задачам отдавать приоритет и как осуществлять менеджмент качества и экологических аспектов операций противоминной деятельности. Исходной точкой для действенного управления рисками является осведомленность о его важности и непрерывное сопоставление со всеми каждодневными действиями, предпринимаемыми руководителями противоминной деятельности. Настоящий стандарт направлен на повышение осведомленности руководителей противоминной деятельности и предоставление инструментов, с помощью которых они могли бы идентифицировать, оценивать, контролировать и анализировать риски в своих различных многочисленных сферах ответственности. В приложении B к настоящему стандарту представлены руководящие указания в отношении применения инструментов для выявления, оценивания и анализа рисков.

В системе ISO риск определяется как «влияние неопределенности на выполнение целевых задач», то есть там, где есть неопределенность, там есть и риск. И наоборот: там, где есть знания, есть и доверие, а неопределенность и риск снижаются. В определении дается указание на важнейший способ снижения риска: через сбор, анализ и обмен информацией. Надлежащее управление информацией является основополагающим для действенного управления рисками.

Принципы и процессы, описанные в настоящем стандарте IMAS, применимы к любым ситуациям, когда руководители противоминной деятельности должны принимать решения в отношении выполнения целевых задач, удовлетворения требований, высвобождения земель и сохранения доверия ключевых участников. В некоторых конкретных ситуациях аспекты управления рисками диктуются существующими документированными источниками. Самые характерные из них относятся к требованиям международных договоров: Конвенции о запрещении противопехотных мин (APMBC), Конвенции о кассетных боеприпасах (CCM) и протокола V к Конвенции о конкретных видах обычного оружия (CCW). Вопросы в отношении приемлемости остаточного риска непосредственно разъясняются в соответствующем тексте, где формируются четкие основы, на которые должна опираться работа руководителей противоминной деятельности. Эти договоры формируют часть массива рамочных документов, которые должны приниматься во внимание руководителями противоминной деятельности при создании действенной системы управления рисками.

Управление рисками, как и большинство других систем менеджмента, не является само по себе сложным или трудным в реализации (хотя в крупных организациях система управления рисками может получить широкое распространение и потребовать большого внимания со стороны руководства высокого уровня). Оно опирается на многократное, последовательное и полномасштабное применение простых принципов и процессов на всех уровнях организации. Все другие аспекты управления, используемые в рамках системы IMAS, включая менеджмент качества, обеспечение безопасности и охраны труда, экологический менеджмент и управление информацией, основаны на применении базовых принципов и процессов управления рисками. Эффективные и результативные руководители, независимо от сферы их ответственности, демонстрируют столь же высокие показатели эффективности и результативности в управлении рисками.

Система IMAS предоставляет основу для разработки национальных стандартов противоминной деятельности (NMAS), но каждый из ее стандартов сам по себе может использоваться как самостоятельный стандарт и предоставлять организациям по противоминной деятельности исходные данные для разработки их собственных политик, процессов и процедур. Руководящие указания, представленные в таком стандарте, будут применимы для всех организаций противоминной деятельности на всех уровнях.

Преобладающие обстоятельства и условия определяют как содержание выполняемых работ, так и скорость реагирования, которую обязана демонстрировать система управления рисками, чтобы оставаться действенной. Быстрое изменение обстоятельств требует от систем управления рисками (как в случаях, связанных с некоторыми ситуациями, когда обнаруживаются самодельные взрывные устройства (СВУ)), чтобы эти системы могли адаптироваться, обновляться и развиваться с очень высокой скоростью. Другие системы могут сохранять соответствие требованиям в течение более длительных периодов без какой-либо потребности в существенных изменениях. В каждом случае система управления рисками остается действенной, только если достаточно часто пересматривается и обновляется, гарантируя отражение всех существенных изменений в окружающих условиях по мере их проявления.

Данный стандарт нацелен на предоставление руководителям противоминной деятельности на всех уровнях необходимых руководящих указаний для выявления рисков в связи с выполняемой работой и сферой ответственности, а также для управления этими рисками. Он основан на руководящих указаниях, приведенных в стандарте ISO 31000 «Управление рисками. Руководящие указания и их адаптация в целях отражения характера рисков в секторе противоминной деятельности».

Управление рисками в противоминной деятельности

1 Назначение

В этом стандарте представлены руководящие указания по внедрению общепринятых принципов управления рисками, практических методов и процессов для программ и организаций по противоминной деятельности.

В первую очередь он предназначен для применения национальными органами противоминной деятельности (NMAA) и национальными центрами противоминной деятельности (MAC), но при этом его основные принципы сохраняют свою силу и могут использоваться и внедряться организациями по противоминной деятельности.

Данный стандарт должен использоваться совместно с такими стандартами, как IMAS 07.12 «Менеджмент качества в противоминной деятельности» и IMAS 07.40 «Мониторинг организаций по противоминной деятельности».

2 Справочные документы

Перечень нормативных справочных документов приводится в приложении A. Нормативные справочные документы — это те документы, которые упоминаются в настоящем стандарте и представляют собой неотъемлемую часть настоящего стандарта.

3 Термины, определения и сокращения

Полный глоссарий терминов, определений и сокращений, используемых в серии стандартов IMAS, приведен в IMAS 04.10.

В серии стандартов IMAS слова shall (должен), should (следует) и may (может) используются для обозначения предполагаемой степени соответствия требованиям. Такое применение согласуется с терминологией, принятой в стандартах и руководствах Международной организации по стандартизации (ISO):

а) глагол shall (должен) используется для обозначения требований, методов или технических условий, подлежащих применению, для того чтобы обеспечить соответствие требованиям стандарта;

б) глагол should (следует) используется для обозначения требований, методов или технических условий, выполнение которых является предпочтительным;

в) глагол may (может) используется для обозначения возможного метода или образа действий.

Термин National Mine Action Authority (Национальный орган противоминной деятельности), или NMAA, означает государственную организацию в стране, подвергшейся воздействию мин. На эту организацию возлагается ответственность за регулирование, управление и координацию противоминной деятельности.

Примечание. В отсутствие NMAA ООН или иной признанный международный орган может принять на себя некоторые или все такие обязанности, а также осуществлять некоторые или все функции NMAA.

Mine action organisation (Организация по противоминной деятельности) — это «любая организация (правительственный орган, военное ведомство, коммерческая организация или НГО / организация гражданского общества), ответственная за осуществление проектов или выполнение задач противоминной деятельности. Организация по противоминной деятельности может выступать в роли головного подрядчика, субподрядчика, консультанта или агента» (IMAS 04.10).

Термин Risk (Риск) определяется как «влияние неопределенности на выполнение целевых задач» (ISO 31000:2018). Риск можно выразить через источники риска, возможные события, их последствия и вероятность реализации.

В общем случае управления рисками термин «остаточный риск» означает «риск, остающийся после обработки риска» (ISO 27001:2013)

С точки зрения технического аспекта противоминной деятельности термин «остаточный риск» означает «риск, остающийся после применения всех разумных усилий, направленных на выявление, определение и устранение всех явных и предполагаемых боеприпасов взрывного действия посредством нетехнической и технической разведки обстановки и/или проведения очистки» (IMAS 04.10).

Термин Context (Обстановка) подразумевает «сочетание внутренних и внешних проблем, которые могут оказать влияние на подход организации к разработке и выполнению целевых задач» (ISO 9000:2015).

Internal context (Внутренняя обстановка) — это «параметры и факторы, находящиеся в сфере компетенции внутреннего органа принятия решений и в диапазоне возможностей данной организации, влияющие на постановку целевых задач и их выполнение. К таким параметрам и факторам относятся внутренние ключевые группы в организации, подход к общим процессам управления, договорные отношения, потенциал, культура и стандарты. Понятие Governance (Общий процесс управления) включает в себя организационную структуру, политики, целевые задачи, роли, отчетность, процессы принятия решений и потенциал, включая знания и человеческие, технологические, финансовые и системные ресурсы».

Примечание. Руководящие указания, направленные на уяснение и определение внутренней обстановки в организации, представлены в разделе 7.1.1 настоящего стандарта.

External context (Внешняя обстановка) определяется как «местные, национальные и международные параметры и факторы, влияющие на постановку и выполнение целевых задач и выходящие за пределы исключительной сферы компетенции органа принятия решений в организации, куда относятся, помимо прочего, внешние ключевые участники, их ценности, взгляды и отношения, а также ключевые движущие силы и важные тенденции в социальной, культурной, политической, профессиональной, законодательной, регуляторной, технологической, экономической, природной и конкурентной среде».

Примечание. Руководящие указания, направленные на уяснение и определение внешней обстановки в организации, представлены в разделе 7.1.1 настоящего стандарта.

Термин All reasonable effort (Все разумные усилия) «описывает считающийся минимально допустимым уровень усилий по выявлению и документированию загрязненных участков или по устранению присутствия боеприпасов взрывного действия либо подозрений в отношении такого присутствия. Все разумные усилия считаются уже предпринятыми, если затраты на выделение дополнительных ресурсов рассматривается как нецелесообразные в сопоставлении с ожидаемыми результатами» (IMAS 04.10).

Термин Risk treatment (Обработка риска) означает «выбор и реализацию вариантов действий по урегулированию риска». Термин «обработка риска» в противоминной деятельности может также заменяться терминами «смягчение риска» или «снижение риска».

Risk control (Контроль риска) — это «меры, позволяющие удерживать риск на определенном уровне и/или изменять его» (ISO 31000:2018). В противоминной деятельности контроль риска — это, как правило, действие, направленное на снижение/смягчение риска.

Risk evaluation (Оценивание уровня риска) — это «процесс, основанный на анализе риска, для определения того, был ли достигнут приемлемый уровень риска» (IMAS 04.10).

Improvement (Совершенствование) — это «деятельность, направленная на повышение производственных показателей» (ISO 9000:2015).

Stakeholder (Ключевой участник) — это «лицо или организация, которые могут оказывать воздействие или находиться под воздействием либо воспринимать себя как подвергшихся влиянию каких-либо решений или действий» (ISO 31000:2018).

4 Целевое назначение

Целевым назначением управления рисками в противоминной деятельности является выявление, оценивание, контроль и критический анализ риска на тот момент, когда он может возникнуть, чтобы таким образом программы, проекты и мероприятия противоминной деятельности могли осуществляться безопасно, действенно и эффективно и обеспечивали выполнение поставленных перед ними целевых задач.

5 Принципы и основные вопросы

5.1 Важность систем управления рисками

Управление рисками является принципиальным моментом для всех программ противоминной деятельности. Помимо других аспектов, оно помогает руководителям и другим сотрудникам обеспечить:

- более точное выявление благоприятных возможностей и угроз в отношении организационных инициатив;

- соответствие требованиям действующего законодательства;
- совершенствование потенциала в проведении переговоров / обсуждений стандартов;
- боле высокий уровень открытости и прозрачности принимаемых решений и оперативного управления;
- усовершенствованный процесс борьбы с потерями, снижение ущерба от потерь/происшествий и стоимости риска;
- контроль над коммерческими страховыми взносами/выплатами;
- изучение приобретенного опыта и вынесенных уроков из успехов и неудач;
- избежание дорогостоящих непредвиденных событий за счет выявления рисков на ранних этапах и управления ими;
- совершенствование общего управления программами и защиты на уровне организации;
- повышение уровня доверия со стороны заинтересованных участников и совершенствование возможностей по привлечению ресурсов;
- более обоснованные базовые параметры для планирования посредством структурированного рассмотрения ключевых рисков;
- более действенное распределение и эффективное использование ресурсов;
- совершенствование коммуникаций и консультаций как на внутреннем, так и на внешнем уровне.

5.2 Лидерство и заинтересованность

Все системы менеджмента полагаются на четкие свидетельства поддержки и заинтересованности со стороны высшего звена руководства. Конкретные сферы ответственности национальных органов противоминной деятельности (NMAA), центров противоминной деятельности (MAC), организаций по противоминной деятельности, доноров и других соответствующих ключевых участников определены в разделе 8 настоящего стандарта.

5.3 Уместная, исчерпывающая и всесторонняя система

Следует позаботиться о том, чтобы система управления рисками:

- была уместной в обстановке мероприятий противоминной деятельности и отвечала ожиданиям ключевых участников;
- отражала стремление к выполнению обязательств по действующим международным договорам;
- носила всеобъемлющий характер и отражала все типы рисков, связанных с программой, проектом и организацией по противоминной деятельности и обстановкой, в которой она функционирует;
- своевременно и надлежащим образом реализовала усовершенствования в интересах ключевых участников с учетом их знаний, взглядов и восприятия событий.

5.4 Коммуникации и консультации

Следует позаботиться о том, чтобы система управления рисками:

- основывалась на знаниях, экспертных навыках и опыте ключевых участников, а также на базах данных и других информационных ресурсах, помогающих в выявлении, анализе и оценивании уровня риска, а также в установлении критериев риска;
- доводила до соответствующих ключевых участников необходимую им информацию, чтобы они были осведомлены и могли действенным образом управлять рисками, относящимися к их собственным работам и сферам ответственности.

Внедрение действенных, актуальных, легкодоступных и интуитивно понятных механизмов обмена информацией, относящейся к управлению рисками, между ключевыми участниками противоминной деятельности является важным аспектом действенного управления рисками в этой отрасли. Органам противоминной деятельности, руководителям и лицам, принимающим решения, следует выполнить все разумные действия совместно со службой управления информацией в противоминной деятельности в отношении внедрения такого механизма.

5.5 Динамичность и способность к реагированию

Следует обеспечить способность систем управления рисками совершенствоваться, корректироваться и реагировать с надлежащей скоростью на изменения во внешней и внутренней обстановке. В определенных чрезвычайных ситуациях или быстро меняющихся обстоятельствах от систем управления рисками в противоминной деятельности может требоваться быстрота функционирования, а также часто может возникать необходимость в завершении цикла выявления, оценивания, обработки и пересмотра рисков в сжатые сроки. Управление рисками часто является первым элементом любой системы менеджмента, который можно использовать как основу в новых обстоятельствах, требующих высокого напряжения сил. Чтобы обеспечить надежность, системы управления рисками в противоминной деятельности должны обладать способностью отвечать на подобные запросы, предоставляя фундамент, на котором будут базироваться все остальные практические принципы принятия административных, логистических и стратегических решений.

5.6 Интеграция

Управление рисками и управление информацией объединены во всех системах менеджмента в единое целое. Имея в своем составе собственные циклические системы менеджмента, они предоставляют фундамент, на котором строятся все остальные системы менеджмента. Наиболее значимыми примерами в контексте противоминной деятельности являются стратегическое управление, управление, основанное на результатах (RBM), менеджмент качества (QM), экологический менеджмент (EM) и управление задачами техники безопасности и охраны труда (OH&SM). Все они являются составными элементами управления рисками, которое осуществляется при поддержке надлежащего управления информацией.

Стандартные рабочие процедуры (SOP) в противоминной деятельности, а также IMAS и NMAS совместно помогают управлять рисками, связанными с тем, каким образом противоминная деятельность сориентирована, определена и реализована, как осуществляется ее мониторинг и совершенствование, направленные на предоставление ключевым участникам достоверных результатов.

Управление рисками предоставляет важные исходные данные для других систем и, в свою очередь, опирается на информацию, полученную от этих систем, что позволяет обеспечивать уместность, актуальность и действенность. Результативность управления рисками обеспечивается в полном объеме лишь тогда, когда оно интегрировано во все аспекты систем менеджмента противоминной деятельности.

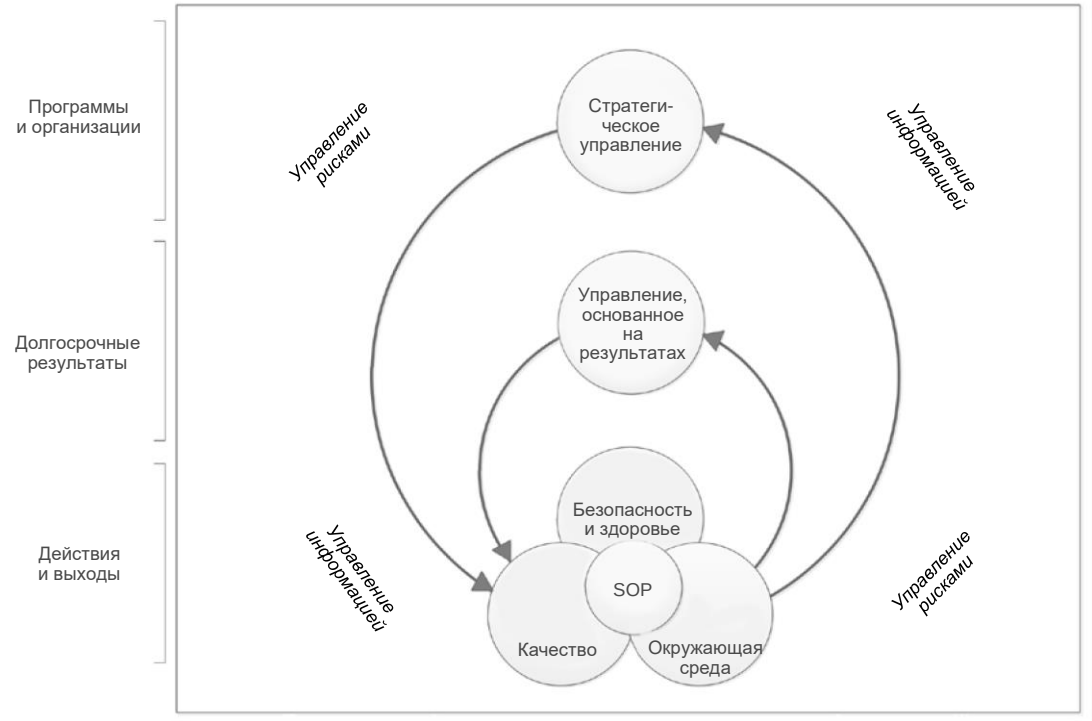


Рисунок 1. Взаимодействие систем менеджмента и процедур на различных уровнях в рамках общей системы управления рисками и управления информацией.

5.7 Управление информацией

Актуальность и исчерпывающий характер управления информацией — это важное условие действенного управления рисками. Своевременное предоставление уместной информации является средством первостепенной важности для снижения степени неопределенности, то есть для снижения риска.

Структура систем управления информацией в противоминной деятельности и их наполнение должны определяться информационными потребностями управления рисками, в том числе сбором соответствующих данных, отчетностью и менеджментом их качества, а также анализом и распространением результатов, относящихся к управлению рисками у ключевых участников.

5.8 Человеческий фактор

Человеческий мозг недостаточно хорошо оснащен инструментами для объективного осмысления больших объемов экспериментальных данных. Влияние инстинктов, привычек и эмоций в большинстве случаев снижает аналитические способности мозга. В результате этого реальная ситуация, являющаяся следствием риска, часто очень существенно отличается от того, как она воспринимается отдельными людьми и группами людей. В процессе управления рисками следует осознавать и делать определенную поправку на ограничения, связанные с человеческим фактором при восприятии риска и реагировании на него. Исследователями из научных и промышленных кругов был определен и изучен диапазон когнитивных искажений. Особый интерес для специалистов по управлению рисками имеют перечисленные ниже факторы.

- **Эвристика доступности** — тенденция в мышлении, предполагающая, что примеры вещей, в первую очередь приходящие на ум (поскольку они необычны, интересны, восхитительны, ужасны и т. д.), обладают большей силой, чем те, которые на данный момент внедрены.
- **Зацикленность на прошлом** — тенденция, связанная со слишком высоким уровнем доверия к старым данным или к одному элементу информации в процессе принятия решений.
- **Предвзятость подтверждения** — тенденция, состоящая в интерпретировании информации определенным образом, позволяющим подтвердить свое предубеждение.
- **Эффект группового давления —** тенденция, состоящая в желании выполнять действия или принимать идеи лишь потому, что много других людей делают это или убеждены в правильности таких идей.
- **Невольное предубеждение** — неосознанное присваивание определенных качеств членам определенной социальной группы.

Другие когнитивные искажения могут оказаться уместными при определенном стечении обстоятельств. Чтобы снизить влияние когнитивных искажений, следует при проведении оценивания и управления рисками в противоминной деятельности всегда отдавать предпочтение количественным данным, если они доступны, и структурированным характеристическим системам, а не опираться на сугубо субъективные мнения людей.

5.9 Возраст, пол и многообразие

Вероятность реализации и последствия различных рисков могут в значительной степени меняться в зависимости от возраста, пола, наличия инвалидности, а также в зависимости от принадлежности к различным этническим, культурным и религиозным группам. Лицам, занимающимся управлением рисками, следует распознавать и принимать во внимание такие различия на этапах выявления, анализа, оценивания уровня и обработки рисков.

Следует накапливать и использовать данные с разбивкой по полу и возрасту (SADD). Это поможет действенным образом выявить, проанализировать, оценить и обработать риски.

При управлении рисками следует позаботиться о том, чтобы женщины, девочки, мальчики и мужчины надлежащим образом привлекались к консультациям и участию в процессах и процедурах в рамках систем управления рисками в противоминной деятельности.

5.10 Непрерывное совершенствование

Следует обеспечить непрерывное совершенствование управления рисками в противоминной деятельности в соответствии с положениями IMAS 07.12 «Менеджмент качества в противоминной деятельности».

5.11 Остаточный риск, все разумные усилия и минимальный практически целесообразный уровень риска (ALARP)

В результате обработки риска (которая подразумевает действия, предпринимаемые в целях снижения, смягчения риска или изменения его уровня иными способами) редко удается достичь его полного устранения. В большинстве случаев после завершения обработки сохраняется определенный уровень риска. Пристегивание ремня безопасности не устранит риск, связанный с дорожно-транспортным происшествием, полностью, но оно существенно снизит уровень такого риска. Заблаговременное согласование с банком курса обмена валюты не исключает риск, связанный с рыночными колебаниями, но обеспечивает сохранение значений в пределах прогнозируемого диапазона. В академическом, научном, государственном и промышленном подходах к управлению рисками, как описано в системе стандартов ISO, «риск, остающийся после завершения обработки», определяется как «остаточный риск».

В контексте процесса высвобождения земель (как описано в IMAS 07.11) «остаточный риск» определяется, в частности, как «риск, остающийся после применения всех разумных усилий, направленных на выявление, определение и устранение всех явных и предполагаемых боеприпасов взрывного действия посредством нетехнической и технической разведки обстановки и/или проведения очистки». Определение, данное в IMAS, полностью соответствует приведенному в ISO. В отношении процессов высвобождения земель следует всегда пользоваться определением, данным в IMAS, тогда как определение, приведенное в ISO, применимо и его следует использовать при описании рисков и управлении ими, когда соответствующие процессы и процедуры не связаны с высвобождением земель в ходе выполнения программ и проектов противоминной деятельности.

Если остаточный риск не является приемлемым для ключевых участников, следует выполнить углубленную обработку с учетом выявления, внедрения и мониторинга согласно положениям раздела 7 настоящего стандарта.

С точки зрения управления задачами обеспечения безопасности можно применять термин ALARP (минимальный практически целесообразный уровень). Применение термина «все разумные усилия» не противоречит по сути достижению уровня остаточного риска, соответствующего ALARP, в процедурах и процессах высвобождения земель.

6 Система управления рисками

Следует позаботиться о том, чтобы по форме и содержанию системы управления рисками в противоминной деятельности отражали обстоятельства и условия, с учетом которых предпринимаются операции противоминной деятельности, а также с учетом уровня сложности организации по противоминной деятельности. В составе любой системы управления рисками в противоминной деятельности следует предусмотреть:

- реестр рисков, в котором регистрировались бы, в том числе, меры по обработке рисков;
- процесс систематического проведения критического анализа;
- предоставление надлежащей профессиональной подготовки для внедрения и сопровождения системы управлениям рисками;
- реестр несчастных случаев, происшествий, частично выполненных задач, несоответствий требованиям и других проблем, связанных с рисками, а также различных событий, в том числе вынесенных уроков из успехов и неудач;
- сопровождение и распространение показателей, относящихся к ведению реестра рисков (с применением данных с разбивкой по полу и возрасту (SADD), если это реализуемо и уместно).

Документацию, в том числе политики, процедуры и записи, следует разработать на уровне, соответствующем сфере охвата системы управления рисками и обстановке, в которой она применяется, а также по мере необходимости поддерживать приемлемый уровень рисков в противоминной деятельности.

7 Процесс управления рисками

Процесс управления рисками является циклическим. Повторяемые итерации процесса:

- обеспечение актуальности системы управления рисками и отражения ею изменений во внутренней и внешней обстановке;
- поддержка непрерывного совершенствования системы управления рисками.

Ключевые элементы процесса управления рисками (см. рисунок 2) таковы:

- уяснение обстановки, в которой осуществляются операции противоминной деятельности; определение объема работ по управлению рисками и установление критериев риска в поддержку надлежащего и действенного процесса принятия решений;
- выявление рисков, связанных с выполнением целевых задач противоминной деятельности;
- анализ выявленных рисков в целях их уяснения и характеризации, а также для установления уровня риска;
- оценивание уровня риска для установления его приемлемости, а также для определения необходимости в обработке риска;
- разработка и внедрение процедуры обработки риска в целях его изменения таким образом, чтобы остаточный риск оставался после обработки на приемлемом уровне;
- пересмотр уровня риска в целях обеспечения актуальности системы управления рисками, ее уместности и действенности.

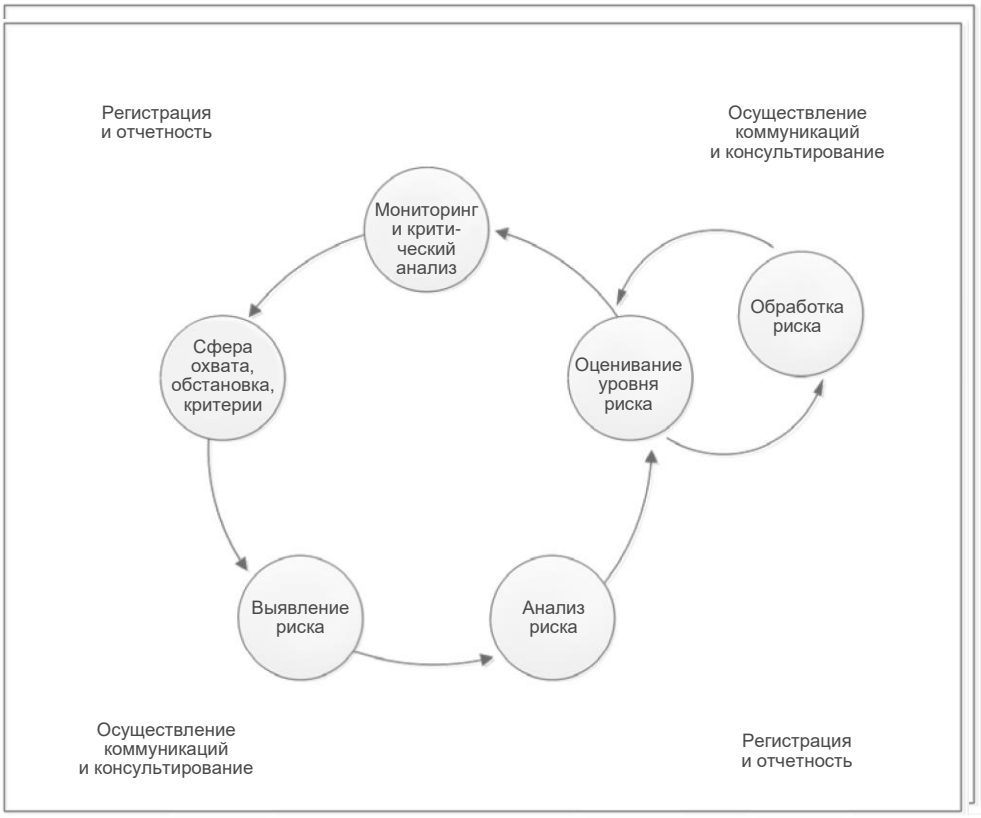


Рисунок 2. Цикл управления рисками в противоминной деятельности

Ключевые элементы цикла управления рисками сопровождаются постоянно осуществляемыми функциями «регистрации и отчетности», а также «коммуникаций и консультаций».

7.1 Обстановка, сфера охвата и критерии

7.1.1 Уяснение обстановки

Обстановка, в которой осуществляется управление рисками, — это внешние и внутренние окружающие условия, где организация по противоминной деятельности ищет пути определения и выполнения своих целевых задач. В быстро меняющихся и чрезвычайных ситуациях способность быстро и точно уяснить обстановку с высоким уровнем достоверности будет крайне важна. Надлежащее распределение ресурсов на раннем этапе в целях обследования, анализа и доведения обстановки — это основная обязанность руководителей противоминной деятельности.

Организациям по противоминной деятельности следует поддерживать актуальность и точность описания обстановки, чтобы риски, которые могут оказать как положительное, так и отрицательное влияние на выполнение целевых задач противоминной деятельности, были выявлены, оценены и обработаны с применением эффективных и действенных методов[1].

В ходе оценивания внешней обстановки организациям по противоминной деятельности следует принимать во внимание, помимо прочего, следующее:

- социальные, культурные, политические, законодательные аспекты, вопросы гендерного равенства и многообразия, нормативно-правовые, финансовые, технологические, экономические и экологические факторы как на международном, так и на национальном, региональном и местном уровне;
- обязательства по международным договорам;
- ключевые факторы роста и тренды, относящиеся к сфере охвата противоминной деятельности;
- отношения с внешними ключевыми участниками, их мнения, ценности, потребности и ожидания;
- договорные отношения;
- сложность сетевой организации и взаимозависимости.

В ходе оценивания внутренней обстановки организациям по противоминной деятельности следует принимать во внимание, помимо прочего, следующее:

- видение, миссию и ценности организации;
- общие подходы к управлению, организационную структуру, роли и отношения подотчетности;
- стратегии, целевые задачи и политики;
- культуру организации;
- окружающую среду, в которой выполняются работы;
- структуру штатного состава, в том числе с учетом гендерной динамики и многообразия;
- стандарты, руководящие указания и методологии, используемые в организации;
- потенциал с точки зрения ресурсов и знаний;
- данные, информационные системы и информационные потоки;
- взаимоотношения с внутренними ключевыми участниками, включая их убеждения и ценности;
- договорные отношения и обязательства;
- взаимные зависимости и взаимосвязи.

[1] Риск, обладающий потенциалом положительного воздействия, может также определяться как «благоприятная возможность».

При оценивании обстановки органам противоминной деятельности и руководителям следует использовать общепризнанные инструменты и технические приемы, включая, помимо прочего, следующее:

- анализ политической, экономической, социальной, технической, законодательной и экологической обстановки (PESTLE);
- анализ сильных и слабых сторон, благоприятных возможностей и угроз (SWOT);
- диаграмму архитектуры противоминной деятельности (подробное описание см. в приложении B);
- выявление ключевых участников и методы анализа (сетка «власть-влияние», диаграммы модели «луковицы», анализ интерфейсов и т. д.);
- анализ аспектов гендерного равенства и многообразия;
- политико-экономический анализ.

7.1.2 Область охвата управления рисками

Область охвата управления рисками в противоминной деятельности должна определяться исходя из нижеследующего:

- объем оперативных, административных и управленческих мероприятий, осуществляемых организациями по противоминной деятельности;
- актуальный и точный анализ внешней обстановки, в которой работает организация по противоминной деятельности;
- актуальный и точный анализ внутренней обстановки в организации по противоминной деятельности;
- потребности, ожидания, требования и предпочтения ключевых участников программы противоминной деятельности.

Область охвата должна быть выбрана с учетом всех рисков, оказывающих воздействие (положительное или отрицательное) на способность организации по противоминной деятельности выполнить целевые задачи.

При определении области охвата управления рисками органы власти / руководители должны учитывать потребность в связях между управлением рисками и другими системами менеджмента, включая стратегическое управление, управление информацией, менеджмент качества, управление вопросами безопасности, экологический менеджмент и управление на основе результатов.

7.1.3 Критерии риска

Критерии риска предоставляют информацию для принятия решений в отношении того, является указанный уровень риска приемлемым или нет. Критерии риска в противоминной деятельности отражают сочетание критериев, принятых на глобальном уровне (таких, например, как соответствие требованиям международных договоров), и критериев, отражающих ценности, политики и целевые задачи конкретных программ, проектов и организаций по противоминной деятельности.

Критерии риска можно установить в договорах, меморандумах о взаимопонимании, стандартах, соглашениях об аккредитации, политиках, процедурах или в других соответствующих документах. Критерии риска следует устанавливать для всех категорий риска, связанных с операциями противоминной деятельности. К таким категориям, помимо прочего, относятся:

- безопасность людей;
- защита физических активов;
- защита и обеспечение сохранности жизней персонала и бенефициаров;
- финансовые прибыли и убытки;
- репутационные аспекты;
- аспекты, связанные с управлением программой и проектом;

- соответствие требованиям международных договоров и выполнение взятых обязательств;
- отношения к ключевым участникам и к общественному мнению (включая «заказчиков»);
- защита окружающей среды;
- менеджмент качества.

Критерии могут быть установлены в численном и/или в описательном виде (например, определения критических несоответствий при высвобождении земель представляют собой критерии риска). Характер риска и неопределенности таков, что определение критериев в абсолютных величинах возможно не всегда. В каждом случае органам власти и руководителям следует искать возможность установления критериев таким образом, чтобы они были максимально понятными, непротиворечивыми и однозначными. Следует позаботиться о том, чтобы критерии не противоречили методам анализа риска, установленным в соответствии с требованиями раздела 7.2.2 настоящего стандарта, и были применимыми для целей оценивания уровня риска, которое описывается в разделе 7.2.3 этого же стандарта.

7.2 Выявление и оценивание риска

7.2.1 Выявление риска

Целью процесса выявления риска является поиск, обнаружение и описание риска, который может воздействовать как положительным, так и отрицательным образом на способность программы, проекта или организации по противоминной деятельности выполнить поставленные перед ними целевые задачи. Следует обеспечить актуальное состояние систем выявления риска и их уместность для применения в преобладающих обстоятельствах и условиях.

Руководителям работ по управлению рисками в противоминной деятельности следует применять общепризнанные методы, инструменты и технические приемы, соответствующие обстановке и сфере охвата их работ по управлению рисками в поддержку обеспечения действенного и всеохватывающего выявления рисков. Такие методы, помимо прочего, включают:

- анализ политической, экономической, социальной, технической, законодательной и экологической обстановки (PESTLE);
- анализ сильных и слабых сторон, благоприятных возможностей и угроз (SWOT);
- мозговой штурм;
- собеседования;
- структурированные технические приемы «что, если...» (SWIFT);
- обсуждения в фокус-группах;
- применение контрольных списков;
- использование результатов расследований по факту несоответствия требованиям, несчастного случая, происшествия и частично выполненных задач;
- использование матрицы последствий и вероятностей;
- анализ трендов в ключевых производственных показателях (KPI).

Риски в противоминной деятельности связаны не только с рисками обнаружения и очистки от опасных предметов. Поскольку высшим приоритетом является обеспечение безопасности затронутых групп населения и персонала, осуществляющего операции противоминной деятельности, способность программ противоминной деятельности выполнить поставленные целевые задачи зависит от большого количества факторов, начиная с поставки оборудования, компетентности руководства и процесса проектирования программ и проектов и заканчивая наличием безопасных/благоприятных окружающих условий при осуществлении работ. В рамках действенного обнаружения рисков в противоминной деятельности следует принимать во внимание зоны неопределенности и риска, связанные со всеми аспектами внутренней и внешней обстановки при проведении каждой работы.

7.2.2 Порядок выполнения анализа риска

Целью анализа риска в противоминной деятельности является уяснение характеристик и природы риска, включая определение его уровня. При анализе риска должны учитываться:

- вероятность возможных событий;
- характер и масштаб/воздействие последствий;
- взаимосвязь между рисками и сложностью взаимодействий;
- близость риска (как скоро он может реализоваться с высокой вероятностью);
- продолжительность действия и изменчивость рисков;
- условия, специфичные для объекта проведения работ или определенных обстоятельств;
- действенность предпринятых мер по контролю риска.

Анализ риска по своему характеру может быть качественным, количественным или полуколичественным. Специалистам по управлению рисками в противоминной деятельности следует работать в тесном контакте со специалистами по информационному менеджменту, чтобы выявлять благоприятные возможности для сбора соответствующих данных, обеспечивающих проведение количественного и статистического анализа риска, когда такие действия реализуемы и эффективны.

Специалистам по управлению рисками следует применять общепризнанные методы, инструменты и технические приемы, уместные для обстановки и сферы охвата их работ по управлению рисками в поддержку действенного и всеохватывающего анализа риска. Такие методы, помимо прочего, включают:

- анализ уровней и трендов в ключевых производственных показателях (KPI);
- использование матрицы последствий и вероятностей;
- структурированные технические приемы «что, если...» (SWIFT);
- проведение анализа по методу «галстук-бабочка»;
- проведение анализа первопричин (RCA).

7.2.3 Оценивание уровня риска

Целью оценивания уровня риска является определение того, находится ли риск на уровне, требующем его обработки для снижения/смягчения до приемлемого остаточного уровня. В целях предоставления информации для принятия решений в отношении приемлемости конкретного риска используются критерии риска.

В результатах установления приемлемого уровня риска может быть отражен набор исходных данных, в том числе:

- исторически применяемые практические методы;
- результаты консультаций с ключевыми участниками, включая различные гендерные группы и группы многообразия;
- ссылки на существующие правовые определения суда;
- требования, задокументированные в международных договорах, соглашениях и других официальных актах международного и национального законодательства.

Результаты оценивания уровня риска могут предписывать:

- отсутствие требований по выполнению дальнейших действий;
- рассмотрение возможности обработки риска;
- проведение углубленного анализа риска для лучшего уяснения сути риска;
- поддержание существующих средств контроля риска;

- рассмотрение возможности корректировки стратегических целей, целевых задач или других аспектов запланированных действий.

7.3 Обработка риска

Целью обработки риска в противоминной деятельности является определение, внедрение и подтверждение результативности действий, обеспечивающих сохранение приемлемого уровня риска.

7.3.1 Варианты обработки риска

Варианты обработки риска описаны ниже.

- **Избегание риска** — отказ от осуществления действия или избегание обстоятельств, которые сопровождаются появлением риска.
- **Устранение источника риска** — выполнение действий, направленных на удаление, уничтожение или изоляцию другим способом источника риска от предпринимаемых действий.
- **Изменение значения вероятности** — осуществление действий по снижению вероятности реализации события, связанного с риском.
- **Изменение последствий** — осуществление действий по снижению воздействия события на людей, активы или на его восприятие.
- **Передача части риска** — наиболее общим случаем является передача части риска посредством внесения соответствующих положений в договоры, бизнес-соглашения, соглашения об объединении усилий или покупку страховки.
- **Принятие риска** как одного из сниженных до приемлемого уровня или для преследования благоприятных возможностей.

Не все варианты обработки риска будут уместны или реализуемы в каждом конкретном случае. Варианты обработки риска необязательно являются взаимоисключающими. Во многих случаях будет уместным сочетать способы обработки.

Применение определенного варианта обработки риска может стать причиной возникновения одного или нескольких новых рисков[2]. Специалистам по управлению рисками в противоминной деятельности следует принимать во внимание возможность формирования новых рисков, когда они рассматривают возможности применения мер по обработке риска.

7.3.2 Остаточный риск и его приемлемость

Концепция «риска, оставшегося после обработки» (как описано в разделе 5.11), — это важнейший компонент любой действенной системы управления рисками.

«Остаточный риск» как «риск, оставшийся после обработки», — это определение и концепция, применимые на любом уровне к любому аспекту управления противоминной деятельностью. Риск является «приемлемым», если ключевые участники противоминной деятельности согласны его принять, поскольку уверены в том, что его принятие выгодно, а также что этот риск надлежащим образом контролируется. В качестве примера из противоминной деятельности: ключевые участники готовы согласиться, что риск является приемлемым для прошедшего обучение и сертифицированного сапера, проводящего операции по очистке, работая в организации с надлежащим менеджментом на правильно управляемом рабочем участке, где применяются утвержденные технологические процедуры и предусмотрено надежное реагирование на возникновение чрезвычайной ситуации. То есть при условии, что меры по обработке риска, его смягчению или снижению приняты как должные и надлежащим действенным образом реализованы, риск, оставшийся после такой обработки (остаточный риск) и связанный с проведением работ по очистке, является приемлемым в сопоставлении с выгодами, получаемыми в этом случае.

[2] В противоминной деятельности наиболее очевидным примером такого принципа является случай, когда во время очистки от мин/ERW с затронутой территории проживания населения устраняется источник риска, но в ходе этого мероприятия создается новый риск для саперов, осуществляющих работы по очистке.

В процессе высвобождения земель концепция остаточного риска обладает достаточной значимостью, чтобы получить свое собственное определение в IMAS 04.10, где определяется как «риск, остающийся после применения всех разумных усилий, направленных на выявление, определение и устранение всех явных и предполагаемых боеприпасов взрывного действия посредством нетехнической и технической разведки обстановки и/или проведения очистки». Предполагается, что там, где были приложены все разумные усилия, остаточный риск будет приемлемым. В данном случае концепция применения «всех разумных усилий» предоставляет организациям по противоминной деятельности и соответствующим учреждениям прямые указания в отношении необходимой формы обработки, которая обеспечит приемлемость остаточного риска. Применяются процессы аккредитации, гарантии качества (QA) и контроля качества (QC), отвечающие требованиям IMAS 07.12, 07.30 и 07.40, чтобы подтвердить применение всех разумных усилий и приемлемость остаточного риска.

Тот же принцип применим ко всем процессам управления рисками. После обработки уровень риска следует оценить и проверить соответствие его уровня установленным критериям (согласно положениям раздела 7.1.3). Если уровень риска после его обработки (остаточный риск) приемлем, тогда дальнейшие действия не требуются. Если выясняется, что остаточный риск неприемлем, тогда органы власти / руководители должны рассмотреть и реализовать другие варианты обработки, продолжая этот процесс до тех пор, пока не будет достигнут приемлемый уровень остаточного риска.

В противоминной деятельности аспекты, относящиеся к остаточному риску и к его приемлемости, также рассмотрены с точки зрения применения требований международных договоров, включая такие:

- Конвенция о запрещении применения, накопления запасов, производства и передачи противопехотных мин и об их уничтожении (APMBC);
- Конвенция о кассетных боеприпасах (CCM);
- Конвенция о конкретных видах обычного оружия (CCW);
- Конвенция о правах людей с инвалидностью (CPRD);
- другие международные договоры и правовые акты, которые могут применяться в зависимости от места, времени и характера мероприятий противоминной деятельности.

Принятие решений в противоминной деятельности опирается на применение принципов и процессов, установленных в настоящем стандарте; в принимаемых решениях должны находить отражение требования применимых международных договоров.

7.4 Владение риском и материальная ответственность

Владелец риска — это ответственное физическое либо юридическое лицо, обладающее необходимыми полномочиями для управления рисками (ISO 27001:2014). Владение риском в противоминной деятельности часто налагается или принимается исходя из исторически сложившихся правил и практик, но также оно может быть определено:

- в описании должностных обязанностей;
- документах по распределению полномочий;
- договорах;
- меморандумах о взаимопонимании;
- соглашениях об аккредитации;
- стандартах и законодательных актах;
- другой оперативной и юридической документации.

Ответственность за обеспечение выявления, оценивания, контроля и критического анализа риска является важнейшим фактором для эффективной системы управления рисками. Оценивание четкости распределения ответственности в управлении рисками на разных уровнях и в отношении различных элементов противоминной деятельности следует рассматривать как неотъемлемую часть процесса оценивания обстановки, который подробно описан в разделе 7.1.2 настоящего стандарта.

Органам противоминной деятельности, организациям и руководителям следует позаботиться о том, чтобы ответственность и полномочия, предоставленные для управления рисками, были четко распределены, а процесс мониторинга подтверждал, что такое распределение является удовлетворительным.

Под ответственностью понимается любой вид правовой ответственности, обязанностей или обязательств, которые могут возлагаться на страну, организацию или отдельное лицо. Ответственность в отношении неблагоприятного события, такого как несчастный случай или обнаружение пропущенного взрывоопасного предмета на участке, связана, как правило, с невыполнением требований согласованной политики или процедуры.

Внедрением всеохватывающей и действенной системы управления рисками следует обеспечить приемлемый уровень рисков, связываемых с юридической ответственностью. Руководящие указания в отношении аспектов риска и юридической ответственности в связи с проведением операций по высвобождению земель представлены в IMAS 07.11.

7.5 Мониторинг

Мониторинг процессов управления рисками следует осуществлять в соответствии с требованиями, изложенными в IMAS 07.40 «Мониторинг операций противоминной деятельности». Показатели результативности применения процессов управления рисками следует установить, поддерживать на должном уровне и вести их мониторинг. К показателям, связанным с риском, можно отнести:

- частоту, тип и уровень тяжести несчастных случаев и происшествий;
- частоту, тип и уровень тяжести несоответствий требованиям менеджмента качества;
- частоту, тип и уровень тяжести несоответствий требованиям экологического менеджмента и происшествий;
- жалобы и другие виды обратной связи от ключевых участников;
- финансовую ценность утерянных, поврежденных и украденных активов;
- отступления от планов в ходе выполнения программ и проектов.

Руководителям противоминной деятельности следует определять и внедрять другие показатели в отношении объема операций, осуществляемых организациями по противоминной деятельности, и обстановки, в которой они выполняются.

7.6 Критический анализ

Критический анализ риска завершает цикл управления рисками и предоставляет основные факторы, определяющие частоту применения функций цикла управления рисками. В обстоятельствах, когда аспекты внутренней и внешней обстановки часто и существенным образом изменялись, следует сократить период между критическими анализами риска.

Критический анализ риска следует проводить в таких случаях:

- в ответ на существенное изменение обстановки;
- в ответ на результаты расследования несчастных случаев, происшествий, частично выполненных задач, результаты анализа первопричин, а также после обнаружения несоответствий предъявленным требованиям и т. д.;
- по истечении соответствующего интервала, определяемого периодичностью в преобладающих обстоятельствах и условиях, но не реже одного раза в год.

7.7 Ведение записей, подготовка отчетности и коммуникации

Системы управления рисками в противоминной деятельности должны обеспечивать ведение надлежащей документации в отношении:

- обстановки, охвата и критериев риска;

- подробных процедур управления рисками;
- записей (в соответствии с положениями раздела 6 настоящего стандарта), подтверждающих, что система управления рисками была внедрена действенным образом.

В документацию могут быть включены политики, процедуры и записи, непосредственно связанные с управлением рисками, а также ссылки на соответствующую документацию, относящуюся к другим элементам комплексной системы управления противоминной деятельностью, в том числе:

- менеджмент качества;
- управление вопросами техники безопасности и охраны труда;
- экологический менеджмент;
- стратегическое управление;
- управление информацией;
- управление, основанное на результатах.

Требования по отчетности в отношении аспектов управления рисками в противоминной деятельности следует детализировать на определенном уровне в следующих документах:

- NMAS;
- соглашениях об аккредитации;
- соглашениях о донорской поддержке;
- SOP организаций по противоминной деятельности;
- в другой соответствующей документации.

Информацию в поддержку непрерывного совершенствования управления рисками в противоминной деятельности следует довести до сведения соответствующих как можно более широких кругов ключевых участников. Эта информация не должна противоречить каким бы то ни было оговоркам, связанным с договорными, коммерческими или другими законодательными ограничивающими условиями.

8 Сферы ответственности

8.1 Национальный орган противоминной деятельности / национальный координирующий орган

NMAA или организация, действующая по его поручению, должны выполнять следующее:

а) в рамках программы противоминной деятельности (MAP) устанавливать, доводить до общего сведения и сопровождать политики, критерии и/или другие руководящие документы в отношении управления рисками в противоминной деятельности;

б) заботиться о том, чтобы организации, выполняющие работы в рамках MAP, внедряли системы управления рисками, которые бы функционировали надлежащим и действенным образом в преобладающих условиях и обстоятельствах;

в) определять национальные стандарты и предоставлять руководящие указания, а также проводить соответствующие мероприятия по управлению рисками для организаций противоминной деятельности;

г) в рамках MAP проводить критический анализ управления рисками с периодичностью, соответствующей преобладающей ситуации, но в любом случае не реже одного раза в двенадцать месяцев;

д) обеспечивать выполнение последующих мероприятий, намеченных в свете выводов и рекомендаций по результатам критического анализа управления рисками в рамках MAP;

е) вести мониторинг результативности управления рисками, осуществляемого организациями по противоминной деятельности, в том числе их подразделениями, в соответствии с IMAS 07.40.

8.2 Организации по противоминной деятельности

Организации по противоминной деятельности должны:

а) внедрять и сопровождать действенное и документируемое функционирование системы управления рисками;

б) внедрять политики, процессы и процедуры управления рисками, соответствующие объемам собственных работ организации и отвечающие требованиям политик в области управления рисками и критериям, установленным NMAA;

в) применять практические методы менеджмента и управления рисками, а также надлежащие рабочие процедуры для обеспечения эффективного и результативного выполнения целевых задач;

г) сопровождать, обеспечивать точность и актуальность документации, предоставлять доступ к ней (в том числе к SOP и другим письменным процедурам) и к отчетам, записям и другим данным о проводимых мероприятиях в соответствии с требованиями IMAS 07.40.

В отсутствие NMAA или подобного органа организации по противоминной деятельности следует принять на себя дополнительные обязанности. К ним относятся:

а) согласование с донорской организацией (либо с клиентом или заказчиком) системы управления рисками в противоминной деятельности;

б) оказание содействия принимающей стране в ходе учреждения NMAA в формировании национальных стандартов по управлению рисками.

8.3 Доноры, клиенты и другие ключевые участники

Данные организации, предоставляющие договоры или финансирующие операции противоминной деятельности, должны:

а) устанавливать и согласовывать свои критерии в отношении управления рисками, а также другие требования к организациям по противоминной деятельности в четкой и недвусмысленной форме;

б) включать в договоры, меморандумы о взаимопонимании и другую соответствующую документацию подробную информацию о требованиях к управлению рисками или (в отсутствие NMAA) о требованиях, установленных ООН либо другим соответствующим международным органом.

Приложения

A. Нормативные справочные документы
B. Инструменты для управления рисками (информативный документ)
C. Руководящие указания по анализу и оцениванию угроз со стороны окружающей среды, затронутой воздействием самодельных взрывных устройств (СВУ)

Приложение A
(нормативное)
Справочные документы

В перечисленных ниже нормативных справочных документах содержатся положения, которые посредством ссылки, приведенной в данном тексте, формируют неотъемлемую часть этого стандарта. Что касается датированных ссылок, то последующие поправки к этим изданиям или их пересмотренные версии являются неприменимыми в данном контексте. Однако сторонам соглашений, основанных на этой части стандарта, рекомендуется рассмотреть возможность применения самых последних изданий указанных ниже нормативных документов. Что касается недатированных ссылок, то они указывают на применение самого последнего издания нормативного документа, на который сделана ссылка. Члены ISO и МЭК ведут реестры действующих в настоящее время стандартов ISO или EN:

а) IMAS 04.10 Глоссарий терминов, определений и сокращений, используемых в противоминной деятельности;

б) IMAS 07.11 Высвобождение земель;

в) IMAS 07.12 Менеджмент качества в противоминной деятельности;

г) IMAS 07.13 Экологический менеджмент в противоминной деятельности;

д) IMAS 07.30 Аккредитация организаций и операций по разминированию;

е) IMAS 07.40 Мониторинг организаций по противоминной деятельности.

Приложение B
(информативное)
Инструменты для управления рисками

В данном приложении представлены краткие руководящие указания в отношении использования ряда наиболее широко применимых и распространенных инструментов для помощи при работе с процессами управления рисками. Доступен также и ряд других инструментов, в связи с чем специалистам по управлению рисками рекомендуется ознакомиться с дополнительными вариантами, используя руководящие указания, приведенные в других публикациях и в интернете, а также применять инструменты, наилучшим образом соответствующие потребностям проектов и программ, в которых они участвуют.

В *ISO 31010:2009 «Управление рисками. Методы оценивания риска»* (находится на рассмотрении в ISO в целях обновления по состоянию на февраль 2019 г.) представлены исчерпывающие руководящие указания в отношении инструментов, их слабых и сильных сторон, а также о порядке их применения.

Инструменты, представленные в настоящем приложении, применимы к различным элементам цикла управления рисками в противоминной деятельности, как показано ниже.

№	Инструмент	Обстановка / объем работ	Выявление риска	Анализ риска	Оценивание уровня риска	Обработка риска	Критический анализ риска
B.1	Реестр рисков	X	X	X	X	X	X
B.2	PESTLE	X	X				
B.3	SWIFT		X	X	X		
B.4	SWOT	X	X			X	
B.5	Архитектура противоминной деятельности	X					
B.6	Матрица последствий и вероятностей			X	X		
B.7	Анализ по методу «галстук-бабочка»			X	X	X	

B.1 Реестр рисков

В реестре рисков представлены основные средства для регистрации выявленных рисков, оценивания их значимости, сведения о мерах по обработке и свидетельства о проведении критического анализа.

Реестр рисков следует сопровождать, как того требуют контролируемые документы согласно положениям раздела 19 стандарта IMAS 07.12.

Руководители противоминной деятельности могут сделать выбор в пользу адаптации и корректировки формата реестра для отражения политик, требований и обстоятельств, относящихся к их организациям по противоминной деятельности, но рекомендуется, чтобы в любом случае реестр рисков содержал как минимум нижеприведенные данные.

- Сведения об организации, программе или проекте, ведущих данный реестр рисков.
- Сведения о лице, отвечающем за действенную реализацию управления рисками, и его должности.
- Дата последнего пересмотра реестра рисков.
- По каждому риску приводятся:
    - идентификационный номер риска;
    - категория риска (например, политический, экономический, связанный с безопасностью, окружающей средой и т. д.);
    - описание риска (например, дорожно-транспортное происшествие, незапланированный взрыв на складе боеприпасов (UEMS) и т. д.);
    - оценка вероятности реализации события риска;
    - оценка тяжести последствий реализации события риска;
    - оценка уровня риска;
    - меры по обработке риска (смягчение, снижение), связанные с этим риском;
    - сведения о лице, отвечающем за действенную реализацию обработки риска, и его должности.
- Дата следующего пересмотра реестра (без учета того, что определенные несчастные случаи, происшествия или другие значительные события могут потребовать переноса пересмотра реестра рисков на более ранний срок).

Организации могут по своему желанию внести дополнительные сведения, чтобы отразить требования своей системы менеджмента организации, а также в целях использования другой общепризнанной системы управления рисками. Некоторые организации по своему выбору включают сведения об уровне риска до проведения обработки риска и после ее завершения.

Следует убедиться, что содержимое реестра рисков не противоречит сфере охвата системы управления рисками согласно определению, данному ответственными специалистами по управлению рисками в противоминной деятельности.

Реестр рисков может представлять собой простую таблицу (в формате текстового редактора или электронной таблицы), динамическую базу данных, либо же он может храниться в специальном приложении для управления рисками, многие из которых доступны на интернет-ресурсах.

Следует использовать дневники или другие постепенно заполняемые системы документирования, чтобы гарантировать проведение критического анализа риска через установленные периоды времени (согласно положениям раздела 7.6 настоящего стандарта).

B.2 Анализ PESTLE

При использовании комплексного и открытого подхода к пониманию внешней обстановки важно, чтобы потенциально значимые, но малоизвестные риски и их источники не были упущены, оставлены без внимания или забыты. Инструмент PESTLE используется для оказания помощи в выявлении внешних факторов воздействия на программу, организацию или проект, а также на решения, которые принимаются в отношении целевых задач и порядка их выполнения. Вот как расшифровывается название инструмента PESTLE.

- **Political (политический)**: относится к национальной, региональной и местной политике (как правительственной, так и учрежденческой и пр.).
- **Economic (экономический)**: относится к коммерции и финансам.
- **Social (социальный)**: относится к местным сообществам, человеческим ресурсам и культурным аспектам.
- **Technical (технический)**: относится к оперативному и технологическому аспектам.
- **Legal (юридический)**: относится к национальному, международному, гуманитарному и другим законодательствам и нормативно-правовым актам, а также стандартам и пр.
- **Environmental (экологический)**: относится к окружающей среде (как природной, так и созданной человеком).

В каких случаях используется этот инструмент

Подход PESTLE может использоваться как вспомогательное средство для напоминающих/контрольных списков, чтобы помочь выявить всех ключевых участников процесса и заинтересованные стороны (как часть описания обстановки, в которой работает организация по противоминной деятельности, осуществляется программа или проект), или как структура для выявления рисков.

Примечание. Анализ PESTLE может также быть полезным в качестве вспомогательного при использовании многих других инструментов менеджмента.

Порядок применения инструмента

Анализ PESTLE может применяться во время групповых собраний, а также в поддержку кабинетных исследований и других видов анализа рисков, систем, конкретных тематических разделов или проблем и событий.

Понимание ситуации / сферы охвата

- Определите, на чем будет сосредоточен анализ (система в целом, разработка нового нормативного регламента, осуществление операций в отдельной организации, мероприятие, задача и т. д.).
- Примите решение в отношении того, потребуется ли разбиение анализа на различные уровни, такие как:
    - локальный, региональный, национальный и международный;
    - стратегический, оперативный и технический;
    - обучение рискам, высвобождение земель, PSSM и т. д.
- Составьте список ключевых участников / заинтересованных сторон / аспектов, относящихся к сфере охвата анализом, каждого из разделов PESTLE.
- Рассмотрите возможность сопоставления дополнительных сведений с каждой из позиций, например таких, как ожидания, требования, предпочтения и т. д.

Выявление риска

- Определите, на чем будет сосредоточен анализ (организационный элемент, действие, элемент оборудования и т. д.).
- Список рисков, соответствующий каждому из разделов PESTLE.

Выгоды и ограничения

Анализ PESTLE представляет собой широко применяемый и простой в использовании способ поддержки пользователей при выявлении и рассмотрении проблем, аспектов и последствий, которые могут выходить за пределы их обычного повседневного опыта или фокуса внимания.

Анализ PESTLE сосредотачивается на внешних окружающих условиях / обстановке и недостаточно хорошо адаптирован к анализу факторов внутри организации. Если сфера охвата недостаточно хорошо определена (а анализ не выходит за рамки сферы охвата), PESTLE может стать громоздким, содержащим излишнюю информацию, которую тяжело проанализировать и уяснить.

B.3 Структурированный технический прием «что, если...» (SWIFT)

Постановка вопросов «что, если...» — это обычная часть многих процессов управления рисками; иногда она является частью более общего процесса мозгового штурма. SWIFT несет в себе более структурированный подход к выявлению и уяснению рисков, чем обычный мозговой штурм. Он позволяет участникам процесса управления рисками мыслить понятиями последствий различных сценариев, которые могут реализоваться для их организации и проводимых ею работ.

В каких случаях используется этот инструмент

SWIFT используется практически во всех вариантах оценивания риска. Он полезен при выявлении риска, анализе риска и оценивании уровня риска. Результаты анализа с использованием SWIFT могут использоваться в качестве информации для разработки мер по обработке риска. SWIFT часто используется в тех случаях, когда требуется учесть последствия изменения ситуации.

Порядок применения инструмента

Определите, какой процесс, процедура или другой аспект подвергаются оцениванию. Прежде чем начнется процесс SWIFT или процесс изучения, назначенный лидер/ модератор готовит список наводящих слов или фраз (которые могли использоваться ранее или формулироваться для отражения особого фокуса процесса). Фразы SWIFT — это фразы, содержащие такие выражения:

- Что, если…?
- Что произойдет, если…?
- Мог бы кто-то или что-то…?
- Кто-то или что-то хотя бы один раз...?

Целью является стимулирование участников процесса SWIFT обыграть возможные сценарии, задуматься над событиями, которые могли бы привести к реализации таких сценариев, а также о последствиях реализации событий риска. В ходе заседания рабочей группы SWIFT следует обсудить и согласовать обстановку, связанную с процессом, процедурой или изменением. После этого модератор ставит участникам вопросы для обсуждения:

- известные риски и опасности;
- предыдущий опыт, в том числе происшествия, несчастные случаи и другие проблемы;
- известные и существующие средства контроля рисков и их результативность;
- соответствующие SOP, средства для напоминания, контрольные списки и другие документированные руководящие указания;
- требования юридических, нормативных документов и стандартов, а также другие связанные с ними требования.

Каждый риск, выявленный участником, суммируется и записывается (можно использовать реестр рисков в формате, рекомендованном в приложении), а также приводится описание причин, последствий и выполненной обработки.

Примечание. Полезными могут оказаться диаграмма Исикавы («рыбья кость») и метод «5 зачем», чтобы исследовать первопричины аспектов выявленных рисков.

Участники процесса SWIFT рассматривают степень действенности существующих средств контроля и, если необходимо, согласовывают план действий (что будет сделано, кем и когда?) по внедрению дополнительных средств контроля. На данном этапе обсуждения может быть полезным продолжение процесса ответов на вопросы «что, если...».

Выгоды и ограничения

Метод SWIFT может быть быстрым и результативным способом фокусировки внимания на существенных аспектах операций и мероприятий. Он гибок и может применяться к различным действиям, процессам, системам и процедурам. Он позволяет руководителям, работникам и другим ключевым участникам использовать свой опыт, а также получить в результате четкий план действий по усовершенствованию процесса обработки рисков.

Преимущества метода SWIFT обычно зависят от способностей лидера/модератора процесса оценивания риска, а также от уровня знаний участников. Если группа не может придумать и задать важные вопросы, возможно, она не замечает важных проблем. Метод SWIFT обычно приносит качественные, а не количественные результаты.

B.4 SWOT-анализ

В каких случаях используется этот инструмент

Анализ сильных и слабых сторон, благоприятных возможностей и угроз (Strengths, Weaknesses, Opportunities and Threats, SWOT) может оказать помощь руководителям противоминной деятельности в уяснении важных аспектов внутренней и внешней обстановки, в которой они проводят свои работы. Усовершенствованный SWOT-анализ может оказать помощь в разработке надлежащих методов обработки риска.

SWOT-анализ лучше всего проводить в группе совместно с представителями как можно более широкого круга ключевых участников.

SWOT-анализ — это важнейший инструмент для процесса стратегического планирования. Он может применяться в различных других организационных и бизнес-процессах, а также в процессах планирования.

Порядок применения инструмента

B4.1 Базовый метод SWOT-анализа обстановки и выявления риска

Сильные стороны

Сильные стороны определяются внутренними факторами. Вопросы, помогающие выявить основные сильные стороны, могут быть такими:

- Какие работы мы выполняем на высоком уровне?
- Какие аспекты из тех, которые мы реализуем, делают нас привлекательными для партнеров, заказчиков, доноров и бенефициаров?
- Имеются ли у нас такие активы и ресурсы, без которых выполнение наших работ невозможно?
- Вклад каких факторов в наш успех является наибольшим?
- Какие преимущества по сравнению с другими организациями мы предлагаем?
- Что в глазах наших ключевых участников выглядит как наши сильные стороны?
- Какие специализированные технические приемы, навыки, оборудование или методологии мы используем?

Слабые стороны

Слабые стороны также определяются внутренними факторами. Вопросы, относящиеся к слабым сторонам, могут быть такими:

- Какие из аспектов деятельности, процессов, элементов требуют безотлагательного усовершенствования?
- Вклад каких факторов в наши неудачи или проблемы является наибольшим?

- Какие ограничения стоят на пути нашего совершенствования, расширения деятельности или дифференциации?
- Какие факторы максимально повлияли на проигрыши тендерных торгов, утрату благоприятных возможностей, заказчиков, доноров и т. п.?

Благоприятные возможности

Благоприятные возможности отражают аспекты внешней обстановки. Вопросы, относящиеся к благоприятным возможностям, могут быть такими:

- Что из того, что мы не делаем на данный момент, можно было бы делать?
- Имеются ли изменения во внешней обстановке, создающие благоприятные возможности?
- Можем ли мы предоставлять помощь другим организациям в выполнении требований, которые создают сложности для них?
- Полностью ли мы оправдываем доверие наших внешних ключевых участников и реагируем на их потребности?

Угрозы

Угрозы являются характерной особенностью внешней обстановки. Вопросы, относящиеся к угрозам, могут быть такими:

- Какие внешние факторы могут воспрепятствовать нашей возможности работать либо на постоянной, либо на временной основе?
- Какие внешние факторы могут усложнить обеспечение эффективности наших работ?
- Имеются ли изменения и тренды в ситуации с безопасностью, которые могли бы помешать или воспрепятствовать нашей способности выполнять работы и достигать поставленных целей?
- Имеют ли место изменения в политических, экономических или юридических перспективах, которые могли бы оказать на нас существенное отрицательное воздействие?
- Имеются ли изменения социального или культурного характера, которые могли бы отрицательно сказаться на нашей способности выполнять стратегические задачи эффективно и/или результативно?

Руководителям противоминной деятельности следует выявлять дополнительные вопросы, относящиеся к сфере охвата выполняемых работ и рисков, ответственность за которые на них возложена.

Результаты SWOT-анализа часто представляются в виде простой матрицы:

	Полезно (с точки зрения выполнения целевых задач)	**Вредно** (с точки зрения выполнения целевых задач)
Внутренние факторы (относятся к организации)	*Сильные стороны:*	*Слабые стороны:*
Внешние факторы (относятся к обстановке)	*Благоприятные возможности:*	*Угрозы:*

B4.2 Расширенный SWOT-анализ и обработка риска

В расширенном SWOT-анализе рассматриваются соотношения между четырьмя его компонентами, чтобы:

- воспользоваться преимуществами, предоставляемыми благоприятными возможностями, используя для этого сильные стороны;
- снизить воздействие слабых сторон, которые могут создать угрозы для существующей реальности.

Результаты такого анализа часто представляются в виде подобной матрицы:

	Сильные стороны	Слабые стороны
Благоприятные возможности	*Как можно использовать сильные стороны для получения преимуществ, предоставляемых благоприятными возможностями?*	*Каким образом можно преодолеть слабые стороны, препятствующие получению преимуществ, предоставляемых благоприятными возможностями?*
Угрозы	*Как можно использовать сильные стороны для снижения вероятности реализации угроз и нанесения воздействия?*	*Каким образом можно преодолеть слабые стороны, которые могут привести к реализации угроз?*

Меры, которые принимаются по результатам SWOT-анализа, представляют собой способы обработки риска. Они снижают вероятность отрицательных событий и повышают вероятность позитивных. Кроме того, они ослабляют отрицательные последствия и способствуют реализации положительных.

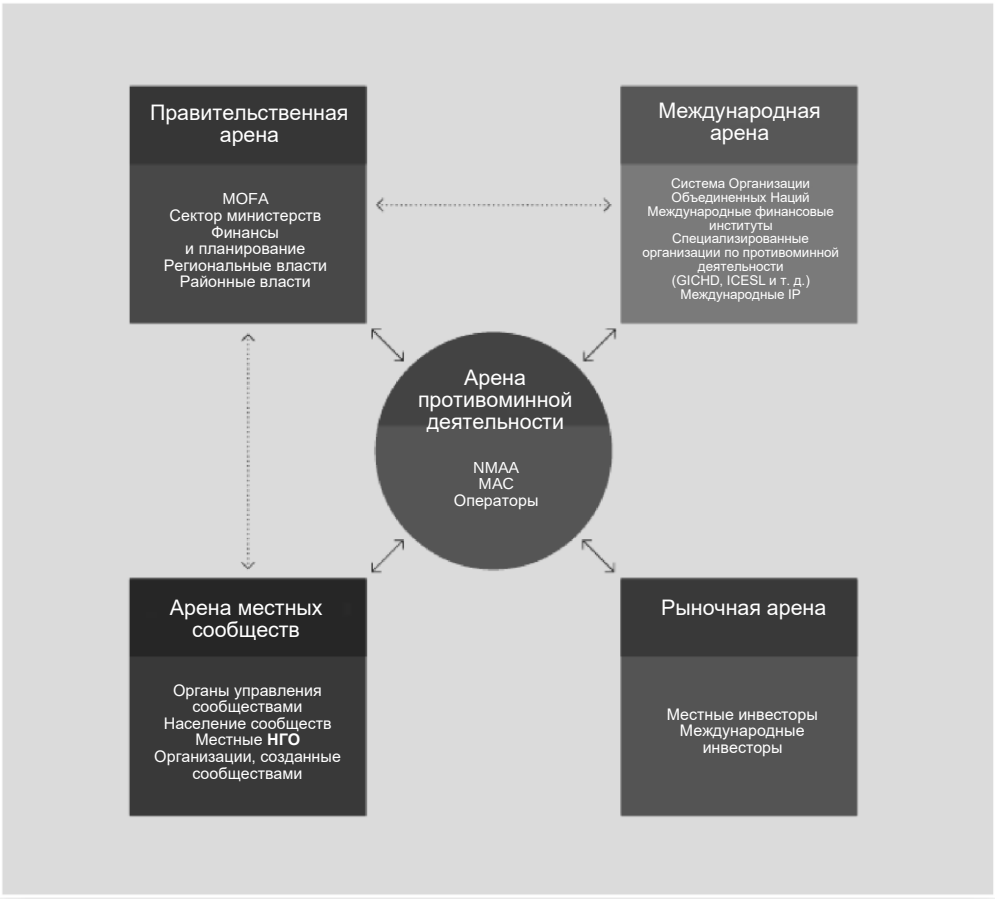
Выгоды и ограничения

SWOT-анализ не вызывает трудностей при его проведении — любой, кто имеет представление о работе организации или о рассматриваемом элементе, может выполнить такой анализ. SWOT-анализ помогает ключевым участникам лучше уяснить суть программы или работу организации, а также внести свой вклад в разработку стратегических целей и целевых задач в поддержку успешных операций, способствующих совершенствованию.

Сам по себе SWOT-анализ не предлагает решения и не указывает приоритеты для действий. Кроме того, имеется риск, состоящий в том, что данный метод может сгенерировать огромный объем информации, причем не только полезной. Нужно, чтобы SWOT-анализ был частью более крупного процесса управления рисками. Могут возникнуть трудности в ходе распределения различных факторов по категориям.

B.5 Архитектура противоминной деятельности

На диаграмме, отображающей архитектуру противоминной деятельности, представлен в сжатом виде обзор основных категорий ключевых участников, связанных с гуманитарной противоминной деятельностью, а также взаимосвязи между ними.



В каких случаях используется этот инструмент

Этот инструмент может использоваться в поддержку специалистов, осуществляющих управление рисками, разрабатывающих планы и проводящих совещания; в целях обеспечения широкого взгляда на проблему выявления ключевых участников в рамках проводимых работ по оцениванию внешней обстановки, а также при рассмотрении влияния указанных ключевых участников и их восприимчивости в отношении вопросов противоминной деятельности.

Порядок применения инструмента

Предоставьте участникам совещания экземпляры диаграммы архитектуры противоминной деятельности и попросите их определить соответствующих ключевых участников, характерных для их собственных организаций, программ или проектов, взятых из различных «арен». Результаты можно собирать, используя таблицу с заголовками столбцов в виде названий каждой из арен.

Диаграмма архитектуры противоминной деятельности может использоваться вместе с анализом по методу PESTLE (см. раздел B.2 данного приложения), чтобы выявить и соотнести риски, присущие каждой из арен или отдельным ключевым участникам в рамках каждой арены.

Диаграмма архитектуры противоминной деятельности может быть полезна в качестве вспомогательного инструмента, когда она используется в различных других аналитических работах на стратегическом, оперативном и техническом уровнях, если это полезно с точки зрения стимулирования и удержания широкого взгляда на вопрос.

Выгоды и ограничения

Диаграмма архитектуры противоминной деятельности представляет собой простой инструмент для напоминания/подсказки, используемый руководителями и участниками совещаний при выявлении ключевых участников по всем аспектам работ в секторе гуманитарной противоминной деятельности вместо использования только наиболее известных им вариантов. Это может оказаться особенно полезным не только при осуществлении работ на стратегическом уровне, но и при рассмотрении аспектов, больше относящихся к оперативным или техническим уровням и обладающих потенциалом собственного воздействия либо получения воздействия вследствие проблем, возникающих у ключевых участников за пределами непосредственного поля зрения руководителей.

Эта архитектурная диаграмма отображает верхний уровень гуманитарной противоминной деятельности. Чтобы получить полноценный результат от проведения любого процесса анализа ключевых участников, руководителям и участникам совещания, возможно, потребуется вникнуть в определения различных арен на более детализированном уровне.

B.6 Матрицы последствий и вероятностей

Матрицы последствий и вероятностей (П/В) широко распространены в управлении рисками. В настоящем приложении не требуются и не даются рекомендации в отношении применения приведенных примеров в том же формате, как показано здесь. Специалистам по управлению рисками следует адаптировать этот инструмент таким образом, чтобы он в максимальной степени отражал те обстоятельства и требования, в которых им самим приходится работать.

В каких случаях используется этот инструмент

Матрицы П/В обычно не предоставляют абсолютные показатели уровня риска, но они позволяют определить структуру, в которой различные риски можно сравнивать и ранжировать. Матрицы П/В предоставляют инструмент для отсеивания, применяемый для проведения оценивания уровней только в отношении рисков, требующих дальнейшей обработки, в противоположность тем, для которых это не требуется (поскольку они уже имеют приемлемый уровень). Матрицы П/В позволяют применить в рамках организации общий подход в отношении риска, его оценивания и определения уровня. Следует позаботиться о том, чтобы критерии риска, связанные с уровнем, требующим обязательной обработки, уровнем, который может быть обработан, или уровнем, не нуждающемся в обработке, отражали обстоятельства, присущие для работ, выполняемых организацией, а также ее отношение к указанным рискам.

Матрицы последствий и вероятностей могут применяться к рискам любых категорий (политическим и экологическим рискам, рискам безопасности и т. д.).

Порядок применения инструмента

Структура матрицы П/В

Матрица П/В формируется по двум измерениям. Одно из них — вероятность наступления события, а второе — тяжесть/последствия. Данные измерения могут принимать любые значения уровней, но чаще всего это 3, 4, 5 или 6. Выбранные измерения могут основываться на описательных или численных величинах.

В самой матрице уровни риска определяются для каждого сочетания значений этих измерений. Матрицу можно настроить таким образом, чтобы вес вероятности был больше веса последствий или наоборот, а можно использовать симметричный вес. Уровни риска могут быть связаны с правилами принятия решений в отношении того, обязано ли руководство предпринимать действия, направленные на обработку риска, а также в отношении других факторов, таких, например, как обязательное применение средств быстрого реагирования.

Использование матрицы П/В

В приведенной ниже таблице представлены примеры измерений для матрицы П/В, которые относятся к аспектам безопасности человеческой жизни. Подобные матрицы можно и следует разрабатывать для других категорий риска с применением других измерений как для тяжести риска, так и для вероятности, если это необходимо.

	Тяжесть	**Описание**		**Вероятность**	**Описание**
1	Задержки	Повреждение оборудования, повторное прокладывание маршрутов доступа к участку проведения работ	**1**	Практически невозможно	Практически невозможно предусмотреть реализацию события
2	Незначительные травмы	Царапины и ушибы, незначительные ожоги, растяжения и вывихи, переломы пальцев, головокружение, порезы, ссадины	**2**	Крайне маловероятно	Такое событие никогда не происходило или случалось очень редко. Ожидания в отношении того, что оно реализуется, отсутствуют
3	Одиночные серьезные травмы	Переломы рук, запястий, голеностопного сустава, значительные ожоги, бессознательное состояние, ампутация пальцев, временная потеря зрения/слуха	**3**	Маловероятно	Известны случаи реализации данного события. Мы понимаем, что такое может случиться, но мы не ожидаем реализации этого события
4	Множественные серьезные травмы	Множественные серьезные травмы у одного человека, одна или несколько серьезных травм у нескольких людей	**4**	Возможно	Такое событие реализуется нечасто. Оно может произойти, и это реально
5	Летальный исход	Один смертный случай или небольшое их количество	**5**	Вероятно	Весьма вероятно, что это случится
6	Множественные летальные исходы	Большое количество смертных случаев	**6**	Весьма вероятно	Такое событие реализуется часто. Мы ожидаем реализацию такого события

В некоторых случаях можно связать числовое процентное измерение с вероятностью реализации событий, хотя часто такой вариант невозможен в связи с ситуацией, в которой осуществляется противоминная деятельность. Специалистам по управлению рисками в противоминной деятельности следует поддерживать связь со специалистами в области информационного менеджмента, чтобы выявить аспекты, которые могут быть полезны при выполнении количественного анализа.

Матрица П/В является примером того, как два измерения могут использоваться совместно и увязываться с уровнями риска (низкий, умеренно низкий, средний, умеренно высокий и высокий). Матрицы П/В часто снабжаются цветовой кодировкой, чтобы упростить понимание.

		Вероятность						
		1	2	3	4	5	6	
Тяжесть	1	УН	С	УВ	В	В	В	1
	2	УН	С	С	УВ	В	В	2
	3	Н	УН	С	С	УВ	В	3
	4	Н	Н	УН	С	С	УВ	4
	5	Н	Н	Н	УН	С	С	5
	6	Н	Н	Н	Н	УН	УН	6
		1	2	3	4	5	6	

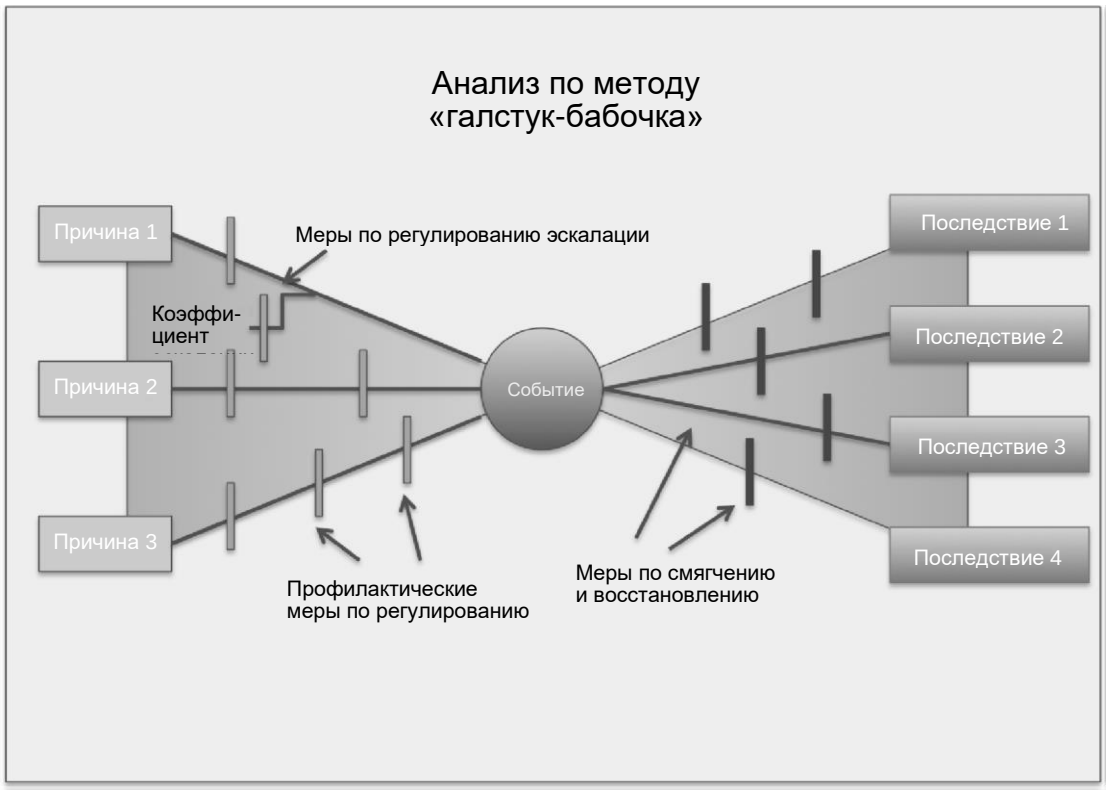
Примечание. Не разработаны стандарты в отношении того, как в рамках матрицы следует распределить уровни значимости. Специалистам по управлению рисками следует согласовать с соответствующими ключевыми участникам подход, уместный для тех обстоятельств и условий, в которых осуществляется их собственная деятельность.

Выгоды и ограничения

Матрицы П/В относительно просты в применении и обеспечивают возможность быстрого ранжирования рисков с учетом различных уровней значимости.

Трудность может вызвать однозначное определение размерностей в матрице П/В, а ее применение может носить субъективный характер. Могут присутствовать различия в результатах, представленных различными людьми или группами при ранжировании одних и тех же или подобных рисков. Матрицы П/В будут различаться в зависимости от организаций их использующих.

B.7 Анализ по методу «галстук-бабочка»



В каких случаях используется этот инструмент

Метод «галстук-бабочка» полезен при анализе событий, которые могут иметь несколько возможных причин, а также ряд последствий.

Порядок применения инструмента

«Галстук-бабочка» — это диаграмма, которая может быть начерчена непосредственно во время сеанса мозгового штурма.

- Для анализа выбирается риск и помещается в точку пересечения отрезков в центре «галстука-бабочки».
- Обсуждаются и описываются перечисленные причины риска (в терминологии безопасности именуемые «опасностями») и механизмы, посредством которых они реализуются и перерастают в риски.
- Линиями соединяются каждая причина и риск.
- Факты, которые могут приводить к эскалации ситуации, также могут быть представлены с левой стороны диаграммы.
- Определяются меры противодействия, которые могут не позволить причине достичь центральной точки-события. Они представляются в виде вертикальных линий, пересекающих соответствующие линии причин.
- Меры противодействия эскалации также могут быть изображены в виде вертикальных линий с левой стороны диаграммы.
- На правой стороне диаграммы представляются последствия, при этом линии последствий выходят из центрального события.
- Меры противодействия, предотвращающие либо смягчающие последствия, отображаются в виде вертикальных линий, пересекающих линии последствий.

Выгоды и ограничения

Анализ «галстук-бабочка» — это удобное и простое для понимания графическое представление риска, его причин, последствий и возможных мер противодействия.

Пользователям следует проявлять аккуратность, чтобы данный анализ не слишком упрощал более сложные ситуации.

Приложение C
(информативное)

Анализ и оценивание угроз со стороны окружающей среды, затронутой воздействием самодельных взрывных устройств (СВУ)

Назначение

Целью данного приложения является определение процессов и выходов, относящихся к реализации анализа и оценивания угроз со стороны окружающей среды, затронутой воздействием самодельных взрывных устройств (СВУ). Анализ угроз будет отражать обстановку на национальном и региональном уровнях и учитывать угрозы, воздействующие на макроуровне. В анализе угроз также будет отражена ситуация в сфере безопасности с участием вооруженных субъектов и их возможностей в отношении СВУ, что поможет субъектам противоминной деятельности в принятии решений относительно потребности в проведении оперативных мероприятий, а также с точки зрения наличия соответствующих условий. Информация для проведения оценивания угрозы предоставляется по результатам углубленного анализа угрозы с отражением конкретных оперативных задач. Будет предоставляться информация как для анализа, так и для оценивания угроз, а результаты будут передаваться в другие процессы IMAS, такие как высвобождение земель (IMAS 07.11) и нетехническая разведка обстановки (IMAS 08.10), если имеются подозрения в отношении присутствия СВУ.

Цель анализа и оценивания угроз

Целью анализа и оценивания угроз является представление ключевым участникам противоминной деятельности актуальных и точных результатов оценивания угроз, присутствующих в окружающей среде, затронутой воздействием СВУ. Результаты этих анализов окажут поддержку в принятии достоверных и действенных решений при планировании стратегических, оперативных и технических мероприятий, а также по вопросам безопасности. Такие оценки также будут использованы в качестве информации для руководителей в отношении долгосрочных рисков для операций, проводимых организациями, а также в отношении их репутации в стране.

Как при анализе, так и при оценивании угроз используются все надлежащие неинтрузивные средства, включая посещение полевых объектов для выявления, сбора, анализа и предоставления информации/свидетельств для формирования краткого описания угроз, которое предназначено:

- для оказания помощи в выпуске общих документов по оцениванию[3];
- для разработки рекомендаций по определению предположительно опасных зон (SHA) и подтвержденных опасных зон (CHA);
- для оказания поддержки в процессе назначения приоритетов;
- для оказания поддержки в исключении и/или дальнейшем сокращении/очищении участков;
- чтобы способствовать действенному и эффективному планированию последующих оперативных технических мероприятий;
- для подготовки информации в целях определения пороговых значения рисков для организации, то есть значений рисков на уровне организации, ниже которых требуется повышение ответственности до уровня NMAA.

Взаимосвязь между анализом угроз, оцениванием угроз и управлением рисками

Риск — это воздействие неопределенности на целевые задачи, в связи с чем при анализе и оценивании угроз используются аналитические методы для управления неопределенностями, связанными с угрозой, и для выбора надлежащих способов реагирования на риск. Как таковые анализ и оценивание угроз являются составными элементами системы управления рисками в противоминной деятельности. Хотя угроза и риск — это близкие по сути явления и часто бывают взаимосвязаны друг с другом, риск является результатом существующей угрозы и вероятностью нанесения урона или вреда. Угрозы могут быть пассивными, но в отношении применения СВУ присутствует злонамеренное человеческое стремление, которое будет оказывать влияние на характер и тяжесть угрозы. На этом отличии делается акцент в различных секторах,

[3] Данный уровень может быть включен в состав оценивания для принятия решения о проведении оперативных мероприятий противоминной деятельности согласно стандарту IMAS 02.10 при первой удобной возможности. Данный процесс также может применяться на национальном, региональном и местном уровнях.

относящихся к различным видам безопасности, как, например, кибербезопасность, исследования в области нераспространения ядерных технологий, а также физическая безопасность.

Ключевые элементы процесса управления рисками (IMAS 07.14, раздел 7), взятые из ISO 31000, также присутствуют в анализе и оценивании угроз (ISO 27001). Каждый процесс фокусируется на этих вопросах на том уровне, который соответствует стратегическим или оперативным целям.

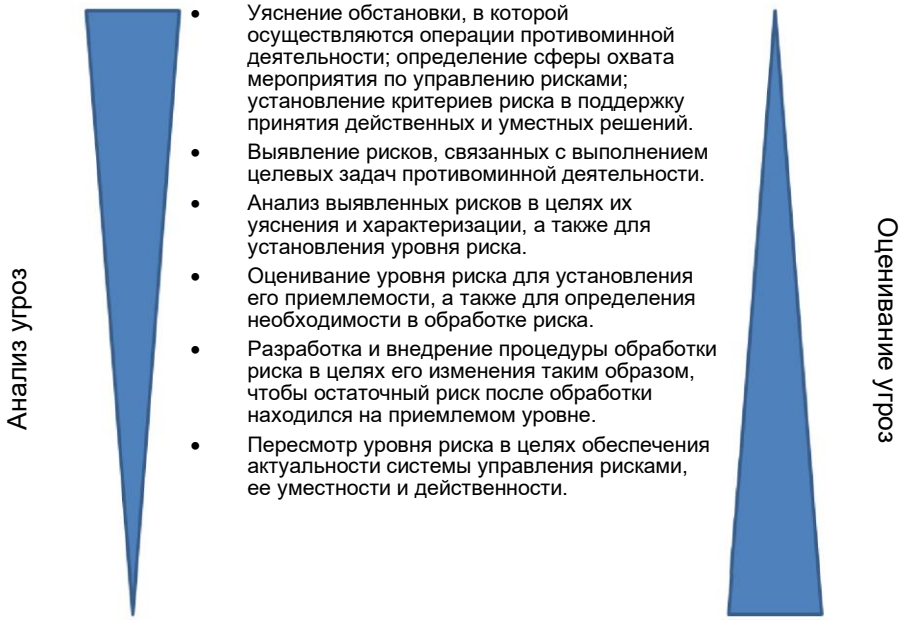


Рисунок 1. Схема типичного распределения усилий в осуществлении процессов анализа и оценивания угрозы по ключевым элементам управления рисками. Здесь предполагается, что анализ угроз осуществляется таким образом, чтобы на этапе оценивания угроз не требовалось возвращаться к более ранним вопросам, подробно изложенным в кратком описании результатов анализа угроз, а можно было непосредственно взять и использовать соответствующие сведения.

Анализ угроз для использования в планировании на национальном уровне

Результаты анализа угроз на национальном уровне следует использовать до того, как будет сформулирована программа противоминной деятельности в определенной стране или регионе, чтобы уяснить оперативную обстановку и предусмотреть возможности для проведения оперативных мероприятий по оказанию гуманитарной помощи, а также для назначения приоритетов задачам. Ширина, глубина и сфера охвата таких аналитических работ на национальном уровне может быть представлена посредством использования подхода PESTLE:

- Какова политическая ситуация в стране и как она может повлиять на противоминную деятельность?
- Какие экономические факторы являются превалирующими?
- Как определяются соответствующие культурные и социальные факторы и чем они обусловлены?
- Какие технологические проблемы затрагиваются?
- Введены ли в действие законодательные акты, регулирующие проведение противоминной деятельности, и требуется ли внесение каких-либо изменений в законодательные акты в том, что касается данного сектора?
- В чем состоят экологические проблемы?

При определении необходимого подхода к обеспечению безопасности и результативности проводимых операций следует учитывать все политические, экономические, социальные, юридические и экологические факторы. Рассмотрение такого разнообразия определяющих факторов позволяет выявить и проанализировать участки, подвергшиеся воздействию. Это воздействие затем можно смягчить посредством применения разрешений, планирования и развертывания ресурсов.

Рисунок 2. Пример элементов, принимаемых во внимание при выполнении анализа угроз на национальном уровне с применением метода PESTLE.

При проведении анализа загрязнения СВУ на национальном уровне используются различные источники информации, предоставляющие в различных объемах исходные данные для применения представленного выше метода PESTLE. Краткое изложение итогов и другие результаты такого анализа будут использоваться как исходные данные для анализа по методу PESTLE, главным образом для технических и других аспектов безопасности с политической точки зрения. Этим будет обеспечена поддержка процесса принятия решений, описанного в IMAS 02.10 «Рекомендации по учреждению программы противоминной деятельности» (раздел 5 «Соображения в отношении учреждения программы противоминной деятельности»).

Если требуются более подробные сведения в отношении СВУ, в ходе проведения анализа угроз могут быть рассмотрены следующие элементы.

Внешние отчеты

Хотя в этих отчетах и не содержатся подробные сведения в отношении конкретных устройств, там может быть приведена ценная информация для предоставления прямых свидетельств в отношении типов таких устройств и их установки. Ниже приводятся примеры, которые могут быть найдены в других организациях, хранящих нужную информацию как для целей анализа, так и для процессов оценивания:

- отчеты о происшествиях со взрывоопасными предметами;
- общие отчеты о состоянии безопасности;
- данные о пострадавших;
- данные о дистанционно доставляемых боезарядах (бомбах, артиллерийских и управляемых боеприпасах);
- этапы конфликта;
- движение ВПЛ/беженцев.

Перечисленные ниже виды информации следует извлекать из доступной отчетности, если это возможно.

- Информация о местоположении, включая GPS-координаты мест происшествия и точек закладки взрывоопасных предметов.
- Фотографии или описания объекта, где имело место происшествие, и нанесенного ущерба.

- Информация о пострадавших, включая их этническое происхождение, гражданство, возраст, пол, вероисповедание, полученные травмы.
- Действия занятых в работах людей, приведшие к происшествию.
- Последняя известная дата о боевых действиях / оккупации вооруженными субъектами.
- Информация о временно перемещенных лицах, включая их этническое происхождение, гражданство, возраст, пол, вероисповедание, причины, по которым они вынуждены были покинуть место проживания, а также то, как с ними обходились различные вооруженные группировки.

Внутренние отчеты

Предполагается, что отчеты этого типа будут храниться и использоваться организациями по противоминной деятельности. Чтобы использовать их при проведении оценки угроз, следует обеспечить доступность таких отчетов для операторов противоминной деятельности в режиме реального времени.

- Связь с сообществом
- Нетехническая разведка обстановки (NTS)
- Локальная задача
- Степень завершения
- Технические отчеты об устройствах

В таких комбинированных отчетах будет содержаться соответствующая информация, позволяющая получить прямые и косвенные свидетельства в отношении типов устройств и местах их установки (в том числе координаты и фотографии). Информация будет крайне уместна по своему характеру, но для этого она должна содержать

подробные сведения о типе устройства и его срабатывании.

- Сведения о 5 основных компонентах СВУ:
  - замыкатель или замыкатели;
  - основной заряд;
  - инициатор;
  - источник питания;
  - контейнер.
- Где устройства были установлены и как они были замаскированы.
- Возможность их срабатывания с течением времени.
- Идентифицирующие признаки, такие как используемый материал.
- Потенциальное нацеливание на лиц, предпринимающих попытки поиска и обезвреживания этих устройств.
- Способность имеющихся в распоряжении процедур и оборудования смягчить угрозу.

Обстановка, в которой воздействует угроза

Анализ угроз предполагает проведение разбивки конфликта в целом на отдельные элементы в целях представления подробной картины угроз в данной ситуации. Хотя этот документ подобен оцениванию угрозы, он представляет более широкую сводку по ситуации конфликта в отношении СВУ, а не суждения, основанные на подробных свидетельствах. Если документ применяется к текущему конфликту, он должен регулярно обновляться, поскольку линии, тактики конфликта и процедуры подвержены изменениям. Любые оценки следует пересматривать после изменения информации, использовавшейся в процессе их подготовки. Ниже приводятся основные разделы информации, которые должны быть рассмотрены при проведении анализа угроз.

Зона географического охвата

Когда конфликты происходят на участках, характеризуемых различными типами окружающих условий, тактика и процедуры задействования ERW, включая СВУ, могут существенно различаться. Такие различия могут оказывать влияние на типы применяемых устройств, их физическое расположение при использовании против различных целей. Для проведения анализа угроз в районах конфликта или в постконфликтных районах следует позаботиться о том, чтобы такой анализ включал географическую информацию на следующих уровнях:

- национальном;
- региональном;
- местном;
- оперативном.

Состояние конфликта

Состояние конфликта важно в случае составления карты угрозы и ее уяснения. Территория может переходить из рук в руки много раз, также со временем могут меняться союзники и зоны внимания вооруженных групп. Это не только имеет прямое отношение к пермиссивности оперативной обстановки, но также предоставляет временные рамки, позволяющие определить с высокой вероятностью, когда последнее СВУ было установлено в определенной географической зоне. Само по себе состояние конфликта не может помочь в определении наиболее вероятного типа устройства, но способствует установлению района, где такие устройства все еще могут оставаться в работоспособном состоянии.

Картографирование угрозы

Картографирование угрозы — это результат передачи информации из сводки по анализу угроз посредством картографирования или спутниковой съемки в целях визуального представления данных при планировании операций. Такие действия могут осуществляться соответствующим органом власти для концентрации внимания на участках, где оператор может реально осуществлять операции по очистке. При этом, если общая безопасность находится на достаточном уровне, имеется возможность сохранять организационное единство операций по очистке. Операторы могут использовать карты и снимки как базовый вариант конфигурации для кабинетного исследования в целях обеспечения безопасности и действенности развертывания группы по проведению разведки обстановки и выполнению задач по очистке. На оперативном уровне их можно использовать как основу, на которой можно базировать разработку подробного оценивания.

Картографирование вооруженных субъектов

В конфликтах, особенно тех, где участвуют одна или несколько негосударственных вооруженных группировок (NSAG), их потенциальные цели могут отличаться в зависимости от района боевых действий и на различных этапах конфликта. В связи с этим критически важно выявить всех государственных и негосударственных вооруженных субъектов, определить намерения/мотивацию каждой из вооруженных группировок и все возможные связи/союзы, которые они могут иметь с другими внутренними или внешними группировками (прохождение информации/технологий). Группировки могут дробиться по этническому принципу, политическим убеждениям, членству в родоплеменных сообществах, вероисповеданию или по языковому принципу.

Замысел

Замысел следует рассматривать на нескольких уровнях, начиная с глобального или национального уровня группировки. На оперативном уровне наиболее важным элементом является влияние на конкретную цель и на то, что будет достигнуто. Мотивация каждого из субъектов конфликта может оказаться недоступной для понимания, особенно при наличии конфедеративных союзов среди участников. В случае более организованных группировок может иметься политическая повестка или криминальный замысел.

Потенциал

Посредством сбора данных из различных источников (обследование жертв, анализ ситуации после взрыва и отчетов с информацией о боезарядах) следует накопить информацию о каждой вооруженной группировке и установить их образ действий, а также следует собрать подробные сведения обо всех принятых в этих группировках процедурах и проводимой тактической подготовке (TTP). Сбор информации часто осуществляется из отчетов о предыдущих атаках и попытках атак, приписываемых вооруженным группировкам или отдельным лицам в составе этих группировок, по найденному оборудованию и фабрикам для изготовления бомб, личным учетным записям и знаниям из доступных ресурсов. Потенциалы каждого из субъектов деятельности будут разными, как и их воздействие в зависимости от того, кто и как будет проводить очистку территорий.

Сводка по результатам анализа угроз

Анализ угроз — это актуализированное разъяснение аналитических результатов, основанное на собранной информации. В него следует включить все выявленные угрозы и наполнить содержанием указанные ниже положения.

- История текущего и предыдущих конфликтов
- Ушел ли конфликт настолько далеко в этом районе в течение соответствующего периода времени, чтобы можно было считать его пермиссивным?
- Определение вооруженных группировок, в отношении которых будет проводиться оценивание

- Определение границ оперативных действий группировки
- Какие группировки при установке устройств производят непосредственное нацеливание, а задействуют их дистанционно?
- Почему они нацелены на индивидуумов или на выявленные группировки?
- Выявление характера устройств, используемых ими для проведения атак
- Использует ли выявленная группировка вспомогательные устройства или последующие действия при проведении комплексных атак?

Ниже представлен рекомендованный шаблон для подготовки сводки по результатам анализа угроз.

(Наименование организации), действующая на ***(вставить наименование территории и ее площадь)*** ищет пути для ***(вставить заявление о миссии группировки)***. На данный момент в этом районе действуют ***(вставить сведения об активных группировках)***. Используемые ими методы выбора целей ***(записать, какие цели они атакуют, то есть патрули / транспортные средства / устройства, устанавливаемые на опорах / где именно (точные данные) / объекты, снижающие скорость / препятствия и т. д.)***. Главной угрозой с высокой вероятностью является ***(указать известные применяемые устройства, то есть инициируемые по проводам (CW) / по времени (TD) / действием жертвы (VO) / по радиокоманде (RC), осколочно-фугасные / зажигательные и т. д. боеприпасы)***. Размеры устройств в диапазоне от ***(указать размеры основных зарядов и типы взрывчатых веществ)***; они помещены в ***(указать упаковку/состав)*** и устанавливаются в ***(указать вероятные места установки)***; предназначены для ***(указать цель / географическую особенность / способ маскировки)***. Методы инициирования, известные по предыдущим случаям применения ***(указать имеющиеся сведения / направленность / минные станции / меры маскировки / длину провода подачи команды управления (CW) / глубину укладки CW / описание компонентов)***. ***(Добавить описание направления размещения минной станции относительно цели вместе с методом и направлением извлечения, если применимо).***

Вторичная угроза: ***(Привести сведения о вторичной угрозе, как, например, нацеливание на персонал групп EOD, сил охраны правопорядка или на персонал групп реагирования в чрезвычайных ситуациях на командном пункте по ликвидации последствий происшествий (ICP). Атаки на цель/охранение и т. д.)***.

Процесс оценивания угроз

Оценивание угроз — это процесс сбора, анализа и интерпретации информации в целях подготовки сводки по угрозе, в которой будут детализированы большинство вероятных типов СВУ, потенциально применимых в конкретном географическом районе. Сюда входит триангуляция имеющейся информации и поиск возможных связей или соотношений между данными, которые на первый взгляд кажутся несвязанными при отдельном рассмотрении. Это процесс исключения, в котором должны учитываться все возможные типы устройств, и, если нет способов, позволяющих их удалять при использовании разумных усилий, такие угрозы необходимо включить в сводку по угрозе. В этом состоит отличие от стандартного подхода к оцениванию риска, которое проводится в ходе процесса высвобождения земель. Различие заключается в уровне анализа, требуемого в соответствии с замыслом и потенциалом благоприятной возможности. В стандартном процессе высвобождения земель и в более стабильных условиях безопасности основное внимание сосредотачивается на риске (или угрозе), создаваемом взрывным устройством, но более широкое оценивание угрозы предполагает также уяснение замысла противоборствующей стороны, причин, которые привели к закладке минного поля или СВУ в определенной части опасной зоны, а также того, в каком месте наиболее вероятным будет обнаружение боеприпасов взрывного действия.

Локальные задачи

Оценивание угроз можно применять к участкам, требующим очистки, или к локальным задачам, в рамках которых тип устройства / подозрительный предмет еще предстоит подтвердить. При этом он может быть установлен таким способом, который не имеет ничего общего с характером установки ранее обезвреженных устройств. В этом случае максимальное внимание сосредотачивается на анализе известных замыслов и полей возможностей, приведенных ниже, а также на применении оценивания не только к известному, но также и к вероятному потенциалу вооруженной группировки, поскольку рассматриваемое устройство может быть новым и ранее не упоминавшимся в отчетах. После этого данная сводка должна использоваться для определения оборудования и процедур, необходимых для проведения безопасной и эффективной очистки. Полученные результаты могут варьироваться, в частности, при проведении работ в различных физических окружающих условиях.

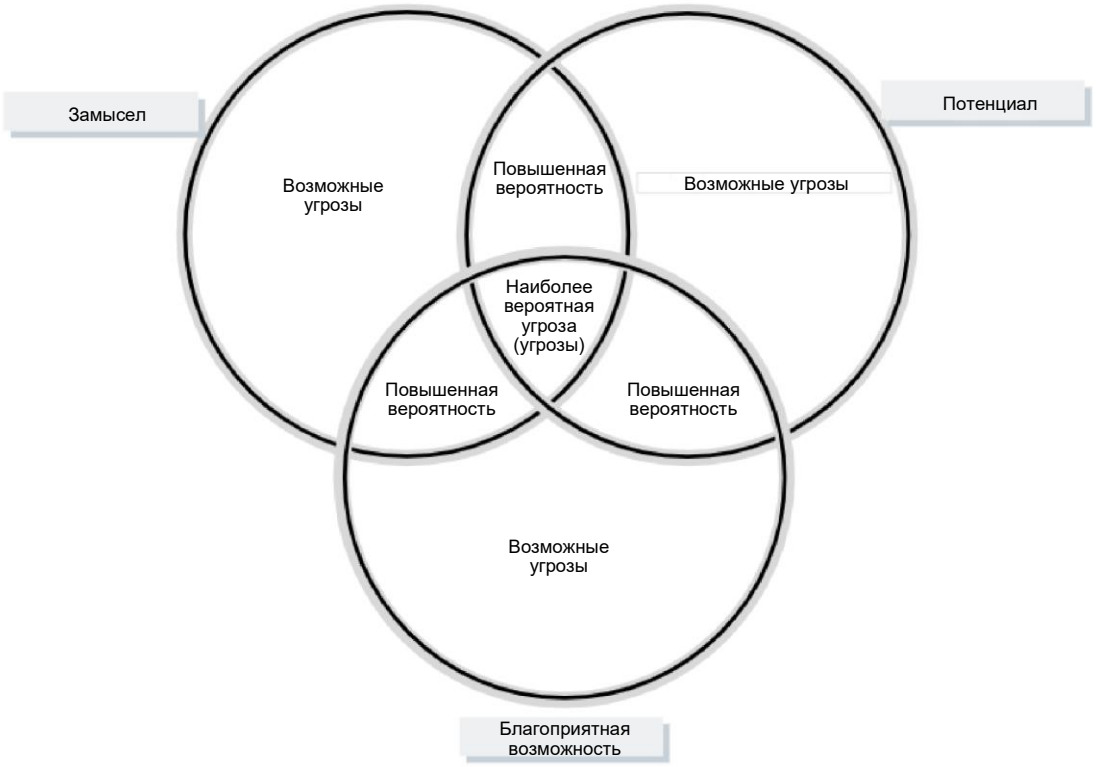


Рисунок 3. Замысел, потенциал и благоприятная возможность

На приведенной выше диаграмме показаны три основных рассматриваемых поля при определении наиболее вероятной угрозы (угроз). Поскольку используются перекрестные ссылки из различных полей, вероятность присутствия устройств конкретного типа повышается.

Замысел

Замысел следует рассматривать с точки зрения вооруженного субъекта, чтобы в максимальном объеме можно было получить указанную ниже информацию.

- Оценивание вооруженных субъектов конфликта: замысел на глобальном, национальном, региональном, местном и оперативном уровнях.
- Уровень приемлемости непреднамеренных жертв.
- Варианты эвакуации: маршруты эвакуации, расстояние от атакуемой цели, позволяющее использовать устройства, управляемые с помощью команд.
- Что было выбрано в качестве цели:
    - силы обеспечения правопорядка, гражданские лица, НГО;
    - здание, инфраструктура, событие.
- Какого эффекта желательно было достичь?
    - Стратегического: устрашения; широкомасштабной поддержки, дестабилизации работы правительства, нарушения безопасной ситуации, общественного резонанса.
    - Физического: убийства, нанесения травм, ущерба, разрушений, введения в заблуждение (в частности достижения общественного резонанса).

Потенциал

Вооруженный субъект может иметь доступ к широкому количественному ассортименту устройств, но будет учитывать эффект, который желательно произвести, то есть выберет лучший тип устройства для достижения такого эффекта. Вооруженный субъект может принять такое решение по результатам изучения поведения цели или оценивания возможных особенностей либо слабых мест. Следовательно, на выбор принципа задействования устройства также повлияют предоставленные целью благоприятные возможности.

- Каким образом они могли бы подготовить атаку?
  - Ресурсы, персонал, подготовка, свобода перемещения, поддержка со стороны местных жителей, способ установки/ маскировки устройства.
- Каким образом они могли бы достичь требуемого эффекта?
  - Порядок срабатывания: по времени, действием жертвы, по команде.
  - Основной заряд: фугасный, осколочный, ударное ядро (снарядо-формирующий заряд, СФЗ), зажигательный, химический, вспомога-тельное устройство (персонал служб экстренного реагирования / специалисты по проведению очистки).

Благоприятная возможность

Благоприятная возможность является жизненно важным элементом при выявлении вероятных участков установки устройств, в частности срабатывающих по времени. Для устройства, срабатывающего по времени, которое предполагается использовать против конкретной цели, должно иметься «окно возможностей», а также цель должна быть на месте в известное время в течение разумного периода, чтобы такое устройство успешно сработало. Для СВУ в целом имеется множество возможностей срабатывания, поэтому анализ особенностей либо слабых мест жертвы, а также окружающих условий будет иметь существенное значение с точки зрения информации для принятия решения о возможном типе инициирующего устройства.

- В каком месте может быть произведена атака (атаки)?
  - Пригоден ли грунт для конкретного типа устройства? Например, мягкий — для нажимных вкладышей; возвышенность — для устройств, срабатывающих по команде.
- Уязвимые участки: дороги, площади, здания, которые используются целью, местность с превалирующими возвышенностями.
- Уязвимые точки: точки въезда/выезда, точки замедления движения, трубы для отвода ливневых вод, мосты, места остановки для отдыха / заправки топливом / обеда / выполнения работ.
- Возможные маршруты эвакуации для вооруженных субъектов после задействования устройства, срабатывающего по команде.
- Когда могут быть совершены атаки?
  - Стиль жизни / график работы.
  - Не только характерные моменты времени (по дороге на работу, с работы, во время работы): когда отворяется дверь, когда человек поднимает лежащий предмет, «во время проведения события».
  - Когда присутствует сама цель?
  - Как долго цель будет находиться в этом месте?

Сводка по угрозе

Когда вся доступная информация проанализирована и оценены наиболее вероятные угрозы, формулируется сводка по угрозе. По результатам оценивания определяется наиболее вероятный тип (типы) устройств, а также места их вероятной установки. Эта сводка также будет полезна при определении параметров очистки и, следовательно, при выборе процедур, которые будут использоваться в ходе очистки. Данную сводку следует пересматривать при внесении любого изменения в оригинальную информацию (независимо от ее источника), если она применяется в ходе оценивания. Это может быть информация, полученная от свидетелей, отчеты или физические данные, разведанные в ходе выполнения задачи.
Структура сводки по угрозе

- Замысел
- Потенциал
- Благоприятная возможность

«Вооруженный субъект, имеющий намерение убить/травмировать гражданских лиц посредством применения самодельного взрывного устройства, инициируемого жертвой (VOIED) (вероятнее всего, это будет самодельное взрывное устройство, срабатывающее от нажимной пластины (PPIED)), установленного в мягком грунте рядом со входом. Оно предназначено для того, чтобы расстроить планы по возобновлению заселения этого участка».

Вооруженный субъект, имеющий намерение повредить либо уничтожить ограниченное количество бронетехники, используемой силами по охране правопорядка, посредством применения самодельного взрывного устройства на растяжке (CIED) (вероятнее всего, это будет самодельное взрывное устройство, инициируемое по проводам (CWIED) с СФЗ) в точке слияния дорог во время движения патруля в целях дестабилизации состояния безопасности.

Цикл управления рисками. Анализ угроз и их оценивание

Цикл управления рисками непосредственно проецируется на анализ угроз и на оценивание угроз.

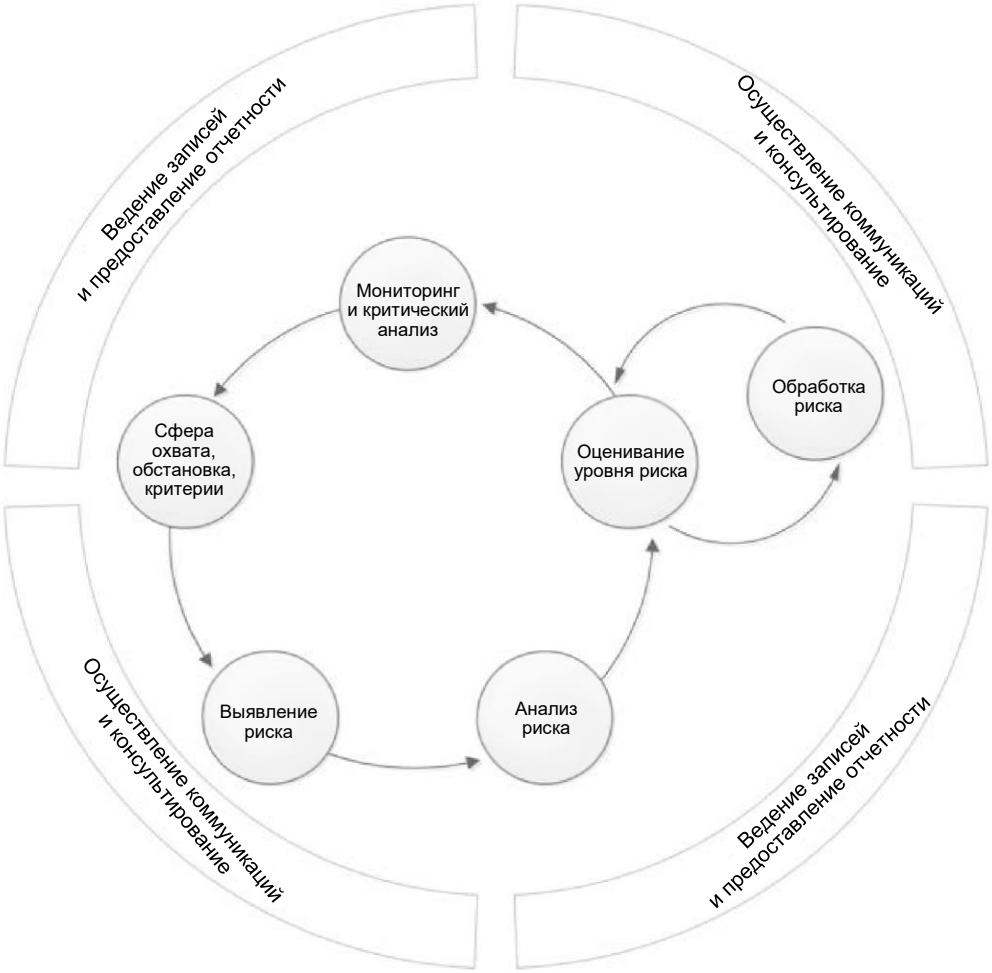


Рисунок 4. Цикл управления рисками

Важным пунктом на этой диаграмме, часто остающимся без внимания, является «Мониторинг и критический анализ». Если риск выявлен, проанализирован, определен его уровень, а после этого не проводится с нужной периодичностью повторный критический анализ, данный факт будет указывать на то, что результат обработки риска мог утратить свою актуальность. В условиях крайне сложной и быстро развивающейся окружающей среды такая ситуация не может сохраняться в ожидании наступления срока проведения критического анализа всех рисков. Как было сказано в описании принципа «Динамичность и способность к реагированию», следует обеспечить способность системы управления рисками совершенствоваться, корректироваться и реагировать с надлежащей скоростью на изменения во внутренней и внешней обстановке. Чтобы этого достичь, необходима ясность в отношении того, какие обстоятельства могут потребовать проведения критического анализа и какие действия надлежит предпринимать, когда возникает эта потребность, чтобы обеспечить завершение критического анализа в уместные сроки. В общем случае критический анализ следует проводить тогда, когда имеют место изменения в информации, используемой в качестве исходных данных для выполнения оценивания.

Увязка со стандартами ISO

Ключевые элементы системы управления рисками взяты из стандарта ISO 31000 «Управление рисками», но ввиду характера рисков, связанных с боеприпасами взрывного действия, включая СВУ и присутствие вредоносных субъектов с их намерениями нанести вред, выявление и анализ рисков более тесно увязываются со стандартом ISO 27001 «Системы менеджмента информационной безопасности».

Оценивание угроз оперативного характера

В качестве приоритетной деятельности организаций по разминированию в период формирования программы противоминной деятельности следует рассматривать проведение анализа угроз на национальном уровне. Такой анализ позволит извлечь важную и уместную информацию из различных источников в отношении угроз, связанных с СВУ. Такая информация может использоваться для углубленного анализа угроз на региональном и местном уровнях. Доступ к результатам такого анализа следует предоставить операторам, чтобы данная информация могла использоваться в ходе оценивания угроз на оперативном уровне.

Оценивание угроз следует использовать в качестве вспомогательных данных для планирования и осуществления всех полевых мероприятий противоминной деятельности, в том числе всех типов разведки и обследования, очистки и мероприятий по вовлечению представителей сообщества. Новая информация в отношении загрязнения боеприпасами взрывного действия (в том числе СВУ) может быть получена неожиданно в любой момент времени в процессе выполнения таких работ, например, от участника мероприятий по обучению рискам. После этого данную информацию можно использовать в качестве исходных данных для процессов анализа угроз и их оценивания.

Оценивание угроз оперативного характера

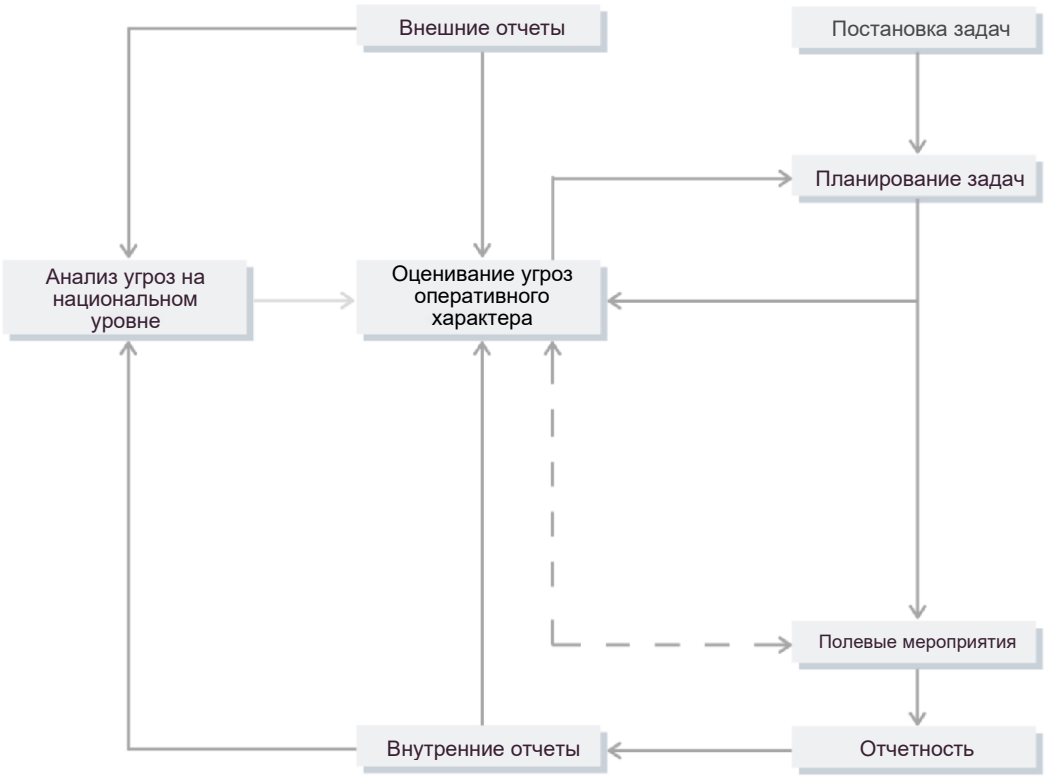


Рисунок 5. Процесс оценивания угроз на оперативном уровне

Кабинетные исследования (как составная часть планирования задач)

Кабинетное исследование представляет собой важнейшую часть планирования задач. Исследование всей доступной документации и проецирование угроз / проблем безопасности осуществляются с целью найти взаимосвязанные элементы информации.

- ГИС.
- Оценивание времени и расстояния для определения возможности или невозможности функциональной реализации.
- Грунт: является ли данный участок пригодным для определенного типа СВУ, включая растительность, сооружения, впадины, возвышенности, участки твердого/рыхлого грунта, известные безопасные маршруты движения, места расположения КПП.
- Этнический/культурный состав, структура гражданства на территории данного района.
- Текущее состояние безопасности, расположение контрольно-пропускных пунктов, мест встречи для постановки задач и работы с сообществом, безопасные маршруты перемещения, активность вооруженного субъекта (всех его группировок), определение гуманитарного пространства.

- Объекты проведения предыдущих работ на данном участке и любые обнаруженные участки с наличием загрязнения.
- Происшествия в связи с подрывом СВУ, имевшие место ранее на данном участке; действия, ставшие причиной происшествия; силы по обеспечению правопорядка; гражданские лица из местных общин; НГО; восприятие непреднамеренных жертв вооруженными субъектами.
- Имевшие место ранее угрозы в связи с наличием СВУ/UXO; технические данные, включая типы устройств, способы задействования и методы установки/маскировки; количество устройств — это информация, необходимая для получения данных о ресурсах, доступных для вооруженных субъектов.
- Выяснение того, что было целью вооруженных субъектов.
- Вторичные опасности (в частности, для инфраструктуры): объекты энергетики, химические производства, замкнутые пространства.
- Хронология конфликта и известные зоны боевых действий или оккупации вооруженными субъектами.

Полевые мероприятия в условиях загрязнения СВУ (нетехническая разведка обстановки)

При проведении нетехнической разведки обстановки (NTS) персонал должен проявлять особую осторожность, особенно на начальном этапе реагирования в рамках гуманитарной противоминной деятельности, поскольку как часть СВУ или как оболочка для него могут использоваться безобидные предметы. Нижеприведенную информацию следует собрать или подтвердить по итогам NTS, включая кабинетное исследование.

- Подтверждение безопасных маршрутов перемещения, границ безопасного участка.
- Прямые и непрямые свидетельства явного или предполагаемого присутствия СВУ.
- Оценивание участка проведения работ, наличие возвышенностей, участков с рыхлым грунтом, растительности, преград; подходит ли участок для установки устройств конкретного типа.
- Дополнительные опасности, такие как замкнутые пространства, выполнение работ на высоте, обращение с химическими реактивами.
- Подтверждение использования зданий и зон до начала конфликта, в период его прохождения и после завершения.
- Повреждения зданий, такие как свидетельства боевых действий, косвенные атаки и возможное загрязнение СВУ.
- 360° за пределами участка выполнения задачи (если применимо) и безопасные условия для съемки и определения опасной зоны.
- Собеседование с владельцем участка и квалифицированным персоналом (инфраструктура), если применимо.
- Собеседование с местными жителями, включая силы охраны правопорядка (если возможно), в отношении состояния безопасности и загрязнения боеприпасами взрывного действия, включая СВУ.
- Применение беспилотных летательных аппаратов для проведения аэрофотосъемки в случае отсутствия доступа на этот участок (может быть интрузивным, если такое решение получит одобрение).