

Управление рисками безопасности

09 июля 2025

Основные идеи

- Процесс управления рисками безопасности (SRM) был запущен в рамках Системы обеспечения безопасности Организации Объединенных Наций (UNSMS) для оказания поддержки учреждениям, фондам, программам и организациям Организации Объединенных Наций в выявлении будущих опасных явлений, которые могут повлиять на достижение целей, проведении оценки вероятности и воздействия этих явлений и определении соответствующих ответных мер в области управления рисками безопасности.
- Процесс SRM позволяет руководителям оценить контекст, в котором ООН осуществляет свои операции, степень, в которой угрозы могут повлиять на персонал, активы, помещения и операции ООН, а также принять соответствующие решения в области управления безопасностью.
- Процесс SRM позволяет пользователям максимально использовать имеющиеся возможности программы и осуществлять программы с приемлемым уровнем риска, а также соответствующим образом распределять необходимые ресурсы.
- Процесс SRM представляет собой структурированный механизм, включающий девять последовательных этапов.

1. Общая информация

Управление рисками безопасности (SRM) представляет собой аналитический процесс, созданный в рамках Системы обеспечения безопасности Организации Объединенных Наций (UNSMS), способствующий выявлению будущих опасных явлений, которые могут повлиять на достижение целей, проведению оценки их вероятности и воздействия, а также определению соответствующих мер реагирования. Он позволяет руководителям оценить условия, в которых действует ООН, степень, в которой угрозы могут повлиять на персонал,

активы, помещения и операции ООН, а также принять соответствующие решения в области управления безопасностью. SRM также обеспечивает проведение детальной оценки рисков для персонала, в том числе связанных с должностными обязанностями лица. Важность SRM подчеркивает тот факт, что за счет выделения соответствующих ресурсов процесс позволяет максимально использовать возможности программ и осуществлять программы с приемлемым уровнем риска.

Данная глава «Руководства по действиям в чрезвычайных ситуациях» предоставляет руководителям и сотрудникам УВКБ ООН техническую информацию по управлению рисками безопасности (SRM) UNSMS. В главе содержатся описания основных концепций и терминологий SRM, включая вопросы, связанные с угрозами, уязвимостью, вероятностью, воздействием и рисками. Цель данного раздела – предоставить руководителям и персоналу знания, которые позволят им влиять на процесс SRM UNSMS, чтобы гарантировать способность УВКБ ООН успешно осуществлять программы, одновременно снижая риски безопасности для персонала, помещений, операций и активов до приемлемого уровня, не мешающего выполнению поставленных задачи. В любых ситуациях руководители должны координировать все этапы SRM со специалистом в области безопасности на местах (FSO), принимающим участие в операции.

2. Актуальность для операций в чрезвычайных ситуациях

В рамках реагирования УВКБ ООН на чрезвычайные ситуации, вероятно, потребуется прибегнуть к специальным SRM для поддержки этой деятельности и/или определения рисков в регионе, где присутствие ООН было ограниченным или не проводилось никаких мероприятий вовсе. Важно осуществлять такие процессы, если в них существует потребность, вне стандартного процесса SRM.

Примечание: в чрезвычайных ситуациях настоятельно рекомендуется сокращать временные рамки, поскольку опасные явления и риск для персонала и операций быстро увеличиваются и, следовательно, могут измениться в короткие сроки, требуя немедленных действий.

3. Основное руководство

Определения:

Угроза: потенциальная причина вреда, созданная преднамеренными действиями. Угроза – это сочетание намерения, возможностей и сдерживающего контекста.

Опасность: потенциальная причина причинения вреда в результате непреднамеренных действий.

Уязвимость: слабая сторона, которая может стать причиной вреда в случае опасности или угрозы.

Риск: сочетание вероятности возникновения опасного события и последствий этого события в случае, если оно произойдет.

Вероятность: оценка вероятности оказания негативного воздействия на организацию потенциальным опасным событием.

Воздействие: оценка потенциального вреда, который событие (если оно произойдет) нанесет организации.

Управление рисками: систематическое определение и внедрение своевременных и эффективных подходов к управлению последствиями угроз для организации.

Предотвращение: принятие мер по снижению вероятности какого-либо события.

Смягчение последствий: принятие мер по снижению воздействия какого-либо события.

Процесс SRM

Процесс SRM UNSMS представляет собой процесс управления рисками, зависящий от контекста, который выявляет события, угрожающие безопасности, и связанные с ними уровни риска, и определяет соответствующие меры управления рисками для структурированного принятия решений о том, какие риски безопасности можно считать приемлемыми. В ходе разработки процесса SRM была обеспечена его динамичность, быстрота реагирования и гибкость, с тем чтобы операции могли приспосабливаться к быстрым изменениям ситуации или контекста в области безопасности и осуществлении программ. SRM также предназначено для учета подходов, ориентированных на отдельные лица (PCA), чтобы гарантировать, что оценки рисков учитывают разнообразные личные профили персонала и определяют дифференцированные, зависящие от контекста риски и меры по их снижению, которые необходимо принять для обеспечения приемлемого для всех участников итогового уровня риска. Подход PCA в рамках SRM обеспечивает операциям благоприятную среду для привлечения персонала с различными профилями и поддержки разнообразных сообществ, которым мы служим, принимая во внимание специфичные для определенного контекста детали.

На уровне операции руководство УВКБ ООН и служба безопасности на местах активно содействуют процессу SRM UNSMS посредством: выявления, определения масштаба и оценки программной деятельности и потенциальной подверженности событиям, угрожающим безопасности, и уровням риска, обеспечения соответствия мер SRM потребностям УВКБ ООН и операции и их практической полезности для организаций, а

также снижения рисков безопасности до уровней, приемлемых для УВКБ ООН. Данный процесс состоит из девяти этапов.

SECURITY RISK MANAGEMENT PROCESS

STEP 1: Geographical scope and timeframe

 Sets the terms of each SRM process by geography and timeframe. For example, a specific SRM may be completed for upcoming elections in a country, or for a specific area of potential vulnerability to be visited by United Nations staff, such as a large refugee camp.

STEP 2: Situational analysis

 Considers political, economic, social and environmental factors in each area, in relation to possible impacts on the safety and security of UN activities.

STEP 3: Programme assessment

 Formally identifies the goals and specific implementation activities of UNSMS organizations in-country.

STEP 4: Threat assessment

 Assesses actors and actions that may cause harm to the UNSMS in the Designated Area, in the categories of armed conflict, terrorism, crime and civil unrest. The intent and capabilities of the relevant threat actors are identified and assessed.

STEP 5: Security risk assessment

 Assesses the different vulnerabilities of the UNSMS presence and activities in-country against the existing threats to determine the likelihood of harmful threat event occurring, and possible impact on UNSMS personnel, assets and operations.



Этап 1. Географический охват и сроки

UNSMS определяет географический охват и временные рамки процесса SRM, выявляя географические местоположения для определения контекста, в котором проводятся оценки программ и уязвимостей. Как правило, территории со схожими характеристиками безопасности следует группировать в пределах общего географического охвата, называемого зоной SRM.

После определения географического охвата важно установить четкие временные рамки для более точного планирования программ, масштабов, охвата, субъектов угроз и, следовательно, вероятности угроз и их влияния на Организацию Объединенных Наций. SRM могут использовать широкий диапазон временных рамок (от нескольких часов и более), однако максимально допустимый срок процесса составляет один год.

Обратите внимание, что в случае подтверждения чрезвычайной ситуации может потребоваться новый процесс SRM, поскольку географическая зона может охватывать территории вне существующих процессов SRM.

Этап 2. Ситуационный анализ

Ситуационный анализ собирает краткую справочную информацию о зоне SRM, позволяющую лицам, принимающим решения в области безопасности, оценить оперативный контекст в различных областях: политике, экономике, экологии, инфраструктуре, силах безопасности, для групп/субъектов, угрожающих безопасности, и в рамках мандата ООН, обеспечивающего принципы безопасности и защиты Организации Объединенных Наций в географическом районе, где проводится оценка.

Это практическое резюме того, как «выглядит» зона SRM и что следует ожидать с точки зрения рабочей среды. Эта часть документа имеет решающее значение для выявления существующих долгосрочных проблем, которые могут создать условия для возникновения угроз.

Примечание о включении подхода, ориентированного на отдельных лиц, в управление рисками безопасности

В разделе анализа ситуации процесса SRM крайне важно проводить исследования соображений, учитывающих отдельных лиц, и предыдущих инцидентов (тенденций) в области SRM и интегрировались эти соображения в нарратив, а именно:

1. Гендерное насилие
2. Восприятие, преследование и насилие в отношении представителей ЛГБТИК+
3. Выявление и дискриминация людей с инвалидностью
4. Племенные, этнические и межобщинные отношения, состав сообщества, представления о различных религиозных группах в зоне SRM
5. Прочие перекрестные факторы, которые могут повлиять на операции или персонал ООН

Понимание контекста и ситуации в зоне CPM, а также возможных существующих тенденций гендерного насилия, дискриминации в отношении определенных категорий персонала, ранее существовавшей напряженности в сообществах является ключевым фактором, позволяющим правильно идентифицировать конкретные угрозы в отношении персонала УВКБ ООН, которые могут быть отражены в части процесса и документации SRM, связанной с оценкой угроз, а также угрозы партнерам и подмандатным лицам, с тем чтобы специалисты по вопросам безопасности УВКБ ООН привлекали соответствующих субъектов и взаимодействовали с другими отделениями в целях поиска мер по смягчению

последствий.

Этап 3. Оценка программы

Оценка программы позволяет специалисту в области безопасности формально понять программные требования организаций UNSMS и выявить программы, которые подвергаются конкретным угрозам. Оценки программы предоставляют общую и конкретную информацию об определенных мероприятиях, проводимых в зоне SRM.

Крайне важно, чтобы страновые операции УВКБ ООН предоставляли актуальную и своевременную информацию в ОЧСБС для проведения точной оценки программы, чтобы UNSMS могла понять масштабы программ и операций УВКБ ООН, а также потенциальные угрозы и риски для персонала, активов, операций и помещений. Помимо этого, некоторые программы могут столкнуться с повышенными рисками.

Например,

- Деятельность УВКБ ООН по мониторингу в области защиты может столкнуться с конкретными угрозами из-за конфиденциальной информации об уязвимых группах населения и действий со стороны субъектов угроз, официальных властей или властей де-факто или негосударственных вооруженных группировок.
- Из-за уникальности оперативной деятельности УВКБ ООН, которая предполагает, что лица, вынужденные покинуть территорию, встречаются с группами по защите в отделениях или помещениях УВКБ ООН, УВКБ ООН сталкивается с повышенной вероятностью насильственных или ненасильственных общественных беспорядков, вторжений в помещения, захвата помещений и т. д.

Примечание о включении подхода, ориентированного на отдельных лиц, в управление рисками безопасности

Часть оценки программ управления рисками безопасности должна также включать ссылку на деятельность УВКБ ООН и других организаций системы управления безопасностью Организации Объединенных Наций, которая может увеличивать подверженность конкретному риску или вероятность нападения, например, мероприятия в области защиты, работа с представителями ЛГБТИК+, кампании вакцинации, расширение прав и возможностей женщин (в патриархальных обществах), а также те ситуации, когда риск могут увеличить определенные характеристики сотрудников (возраст, религия, отличающийся этнический или племенной опыт).

Способность выявлять проблемы, которые могут возникнуть в результате программной деятельности, позволяет уточнить конкретные угрозы на более позднем этапе процесса SRM.

Этап 4. Оценка угроз

Оценка угроз выявляет и оценивает субъектов и действия в географическом регионе, которые потенциально могут нанести вред системе Организации Объединенных Наций.

Оценки угроз также предусматривают деление на общие и конкретные угрозы.

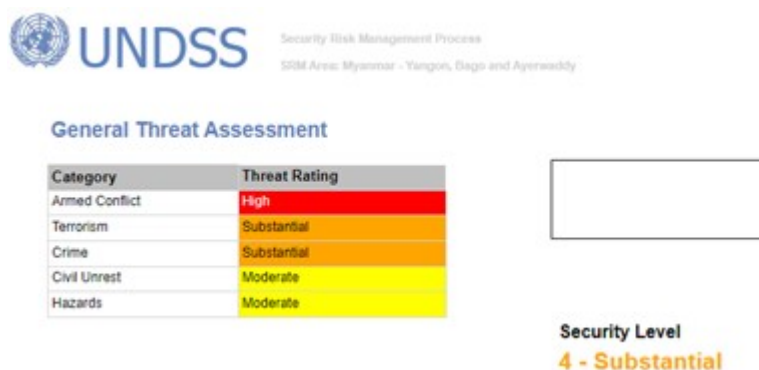
Оценка угроз SRM состоит из двух отдельных частей.

Общая оценка угроз объективно описывает и оценивает угрозы безопасности и опасности в зоне SRM (в UNSMS понятие «защиты» охватывает угрозы, а понятие «безопасность» — опасности. Однако сфера «безопасности» UNSMS не охватывает все непреднамеренные опасные события. В компетенцию UNSMS входят только три области обеспечения безопасности: безопасность дорожного движения, пожарная безопасность и авиационная безопасность.)

Каждая угроза оценивается по шкале от 1 до 5 по трем переменным:

- Намерение: мотивация или склонность субъекта угрозы вызвать угрожающее событие;
- Возможность: способность или возможность субъектов угрозы вызвать угрожающее событие;
- сдерживающий контекст: факторы, не относящиеся к ООН, в географическом регионе, которые препятствуют намерениям или возможностям.

Результатом общей оценки угроз является рейтинг каждого типа угроз или опасностей и уровень безопасности, объединяющий баллы каждой угрозы и опасностей.



Оценка конкретных угроз

Оценки конкретных угроз выявляют определенные угрозы для учреждений, фондов, программ и организаций Организации Объединенных Наций в отдельной зоне SRM. В отличие от общих оценок угроз, которые остаются общими, оценки конкретных угроз выявляют определенные угрозы ООН в целом или угрозы определенному учреждению в зоне SRM.

Для проведения оценки конкретных угроз необходимо подготовить исчерпывающие описания событий, связанные с категорией общих угроз.

Описание события — это четкое описание опасного события, которое будет подробно изучено при оценке риска безопасности для определения уровня риска. Оно должно учитывать негативное воздействие события на организацию и строиться на основе

методологии «кто, что, когда, где и как?»

Примечание: описания событий должны предоставлять достаточно информации, чтобы сузить параметры, позволяя лицам, принимающим решения, оценивать события точнее, чем на основе общей оценки угроз.

- Не все угрозы направлены на Организацию Объединенных Наций. По этой причине в описаниях событий также должно быть указано, является ли угроза «прямой» или «косвенной».
- **Прямые угрозы непосредственно влияют на ООН.** Например, если определенная группа заявила, что она намерена нанести вред ООН, или недавняя история показывает, что ООН является объектом угроз, угрозу следует рассматривать как «прямую».

«Похищение сотрудника Международной организации ООН негосударственными субъектами в пункте X с целью выкупа»

[Что] [непосредственное внимание ООН] [Что] [Кто] [Где]

- **Косвенные угрозы – это угрозы, которые могут нанести вред ООН, однако ООН не обязательно является основной целью.** ООН может быть нанесен вред, если сотрудники или активы ООН окажутся не в том месте и не в то время, будут подвергнуты сопутствующему ущербу, окажутся связаны с основной целью угрозы или, например, если ООН попытается противодействовать.

«Автомобиль ООН поражен самодельным взрывным устройством на дороге X к отделению Y»

[косвенное внимание ООН] [Что/Как] [Где]

Как прямые, так и косвенные угрозы можно разделить на известные и оцененные угрозы:

- Известные угрозы: было сделано заявление о намерении причинить вред ООН или ООН уже был причинен вред.
- Оцененные угрозы: не было заявлено о намерении причинить вред, однако анализы и оценки позволяют предположить, что угроза существует.

После выявления конкретных угроз и согласования описаний событий подготавливается оценка угроз для каждого события, основанная на данных трех переменных: намерении субъекта угрозы/ответственной стороны, возможностях субъекта угрозы/ответственной стороны и препятствующем контексте среды, в которой возникает угроза (например, возможности сил безопасности или отрицательное восприятие таких действий населением). Оценки отдельных угроз подсчитываются так же, как и общие оценки угроз (см. выше).

Примечание: **основывайте свои оценки и решения на данных о риске, а не об угрозе.** В каждой зоне риска безопасности можно выявить серьезную (по своей сути) угрозу, которая, тем не менее, представляет относительно низкий риск для ООН (см. раздел «Риск» ниже).

Примечание о включении подхода, ориентированного на отдельных лиц, в управление рисками безопасности

Крайне важно, чтобы специалисты в области безопасности УВКБ ООН принимали участие в коллективном процессе и обеспечивали полный учет угроз в отношении определенных профилей сотрудников в процессе SRM. Например:

1. Выявляет ли SRM территорию с вооруженными конфликтами, нарушением правопорядка, высоким уровнем преступности или зону, где распространено гендерное насилие?
2. Учитывались ли при выявлении угроз специфичные для контекста показатели или триггеры, связанные с конкретными профилями персонала, находящимися в зоне повышенного риска?

Помимо этого, специалисты в области безопасности УВКБ ООН должны следить за тем, чтобы описания событий основывались на информации об угрозах, собранной и отраженной в ходе предыдущих этапов процесса SRM (т. е. анализа ситуации), чтобы описания событий выявляли угрозы для деятельности, подробно описанной в оценке программы, чтобы описания событий были сформулированы четко и надлежащим образом, чтобы отразить категорию затронутого персонала, их личные профили и субъектов угрозы (кто, что и кем), а также указывать на конкретные места и время, когда и где могут произойти угрожающие события. Это необходимо для разработки соответствующих мер SRM (на более поздних этапах процесса) по снижению вероятности и воздействия угроз.

Этап 5. Оценка рисков безопасности

Оценка рисков безопасности (SRA) определяет и предлагает количественную оценку вероятности и воздействия угроз безопасности, принимая во внимание уязвимость ООН.

Вероятность

В модели SRM вероятность определяется как «оценка вероятности оказания негативного воздействия на организацию потенциальным опасным событием». Она оценивает вероятность того, что произойдет выявленное преднамеренное опасное событие. Идентификатор вероятности является результатом оценки как угрозы, так и мер предотвращения уязвимости.

Меры предотвращения принимаются для снижения вероятности возникновения данного опасного события. Они могут включать, среди прочего, выбор альтернативных маршрутов передвижения, контроль доступа, меры сдерживания, коммуникацию, комендантский час. Для обеспечения эффективности меры предотвращения должны осуществляться до наступления соответствующего события.

Уязвимость к предотвращению определяется как «отсутствие мер предотвращения, призванных снизить вероятность того, что событие произойдет согласно описанию». Поскольку угрозы являются внешними по отношению к ООН, ООН не обладает возможностью их контролировать. Защитить себя удастся лучше всего в случае, если уменьшить уязвимость к предотвращению и тем самым снизить вероятность

возникновения угроз.

Уязвимость к предотвращению оценивается по шкале от 1 до 5 и может быть описана следующим способом:

1. Эффективные меры предотвращения и процедуры управления рисками полностью внедрены и эффективны с течением времени.
2. Эффективные меры предотвращения и процедуры управления рисками полностью внедрены, но демонстрируют одну слабую сторону, которой можно воспользоваться.
3. Меры предотвращения и процедуры внедрены не до конца ИЛИ не всегда эффективны.
4. Меры предотвращения и процедуры внедрены не до конца И не всегда эффективны.
5. Эффективные меры предотвращения и процедуры отсутствуют.

Затем инструмент SRM генерирует рейтинг вероятности путем умножения оценок угроз и уязвимости к предотвращению:

- 1 — очень маловероятно
- 2 — маловероятно
- 3 — умеренно вероятно
- 4 — вероятно
- 5 — крайне вероятно

Воздействие

Воздействие определяется как «оценка потенциального вреда, который событие (если оно произойдет) нанесет организации». Оно охватывает персонал и операции. Сюда также относится способность контролировать или уменьшать последствия события посредством смягчения уязвимости.

Воздействие состоит из трех компонентов:

- влияния на персонал,
- влияния на операции,
- смягчения уязвимости.

Для измерения воздействия на персонал и операции используется шкала от 1 до 5 с соответствующими описаниями.

Влияние на персонал

1. Влияние отсутствует.
2. Незначительный вред.
3. Умеренно травмирующее или травмирующее психологически воздействие.
4. Значительные травмирующие или значительно травмирующие психологически последствия или смертельный исход (один человек или небольшое количество людей).

5. Смертельный исход в масштабах катастрофы (массовые жертвы).

Влияние на операции

1. Влияние отсутствует.
2. Небольшое разрушительное воздействие на программы и/или небольшой ущерб активам.
3. Серьезное разрушительное воздействие на программы и/или значительный ущерб активам.
4. Краткосрочное и среднесрочное приостановление программ.
5. Долгосрочное приостановление или отмена программ.

Смягчения уязвимости

Смягчение уязвимости относится к ситуации «отсутствия контрмер в области безопасности и процедур, предназначенных для снижения воздействия события (если это событие произойдет)». Меры по смягчению последствий – это меры, принимаемые для уменьшения воздействия. Они могут включать эвакуацию раненых (CASEVAC) и [медицинскую эвакуацию](#) (MEDEVAC), сумки для неотложной помощи (ETB) и индивидуальные аптечки первой помощи (IFAK), управление инцидентами с заложниками (HIM), подготовку посредством взаимодействия с правительством принимающей страны, планирование инцидентов с массовыми жертвами, учения, восстановление после бедствия, [планирование непрерывности ведения деятельности](#) и т. д. Несмотря на то, что меры по смягчению последствий направлены на снижение воздействия событий в момент их возникновения и после них, для обеспечения их эффективности планирование и осуществление должны проводиться заблаговременно до наступления таких событий.

Для определения уровня воздействия важно оценить степень осуществления мер по смягчению последствий. Для этой цели в модели SRM применяется шкала от 1 до 5 на основе следующих описаний:

1. Эффективные меры и процедуры смягчения рисков полностью внедрены и эффективны с течением времени.
2. Меры и процедуры смягчения рисков внедрены, но не всегда эффективны или ограничены.
3. Меры и процедуры смягчения рисков внедрены не полностью ИЛИ не всегда эффективны.
4. Меры и процедуры смягчения рисков внедрены не до конца И не всегда эффективны.
5. Меры и процедуры смягчения рисков отсутствуют.

Модель SRM добавляет оценки влияния на персонал и операции к оценкам снижения уязвимости для определения воздействия (влияние на персонал + влияние на операции + снижение уязвимости).

Инструмент SRM автоматически определяет оценку воздействия на основе рейтинга от 1 до 5 следующим образом:

- 1 — незначительное
- 2 — небольшое
- 3 — умеренное
- 4 — значительное
- 5 — критическое

Уровни рисков

Оценка риска объединяет потенциальные будущие опасные события, которые могут произойти, и степень, в которой такие события могут нанести ущерб организации.

Риск = вероятность x воздействие

Risk Matrix		Impact				
		Negligible	Minor	Moderate	Severe	Critical
Likelihood	Very likely	Low	Medium	High	Very High	Unacceptable
	Likely	Low	Medium	High	High	Very High
	Moderately Likely	Low	Low	Medium	High	High
	Unlikely	Low	Low	Low	Medium	Medium
	Very Unlikely	Low	Low	Low	Low	Low

Другими словами:

Risk Score Range	Risk Level
1 to 6	Low
>6 to 10	Medium
>10 to 16	High
>16 to 20	Very High
>20 to 25	Unacceptable

Уровни риска, являющиеся конечными результатами SRA, формируют основу для принятия решений в процессе SRM. Они позволяют лицам, принимающим решения, подготавливать соответствующие стратегии управления рисками и устанавливать приоритеты, пропорциональные уровням риска и связанным с ними описаниям событий.

Примечание: для принятия решений о **приемлемых уровнях риска** необходимо применить самый высокий уровень риска, связанный с любым из событий, к рассматриваемой зоне SRM или программной деятельности.

Этап 6. Измерения SRM

Управление рисками осуществляется путем выявления и внедрения мер SRM, которые

снижают вероятность и/или воздействие за счет снижения уязвимости.

Меры SRM могут быть определены только после оценки:

- сильных и слабых сторон существующих мер предотвращения и смягчения последствий (в отношении конкретных угроз);
- уровней риска, связанных с угрозами и основанных на их вероятности и воздействии.

В контексте вышеуказанных стратегий меры SRM могут использоваться для управления рисками, связанными с выявленными опасными событиями. Оценив уязвимость к предотвращению и смягчению последствий (как описано на предыдущем этапе), специалисты в области безопасности могут определить, какие дополнительные меры (меры, которые в настоящее время не применяются) необходимы, включая меры и процедуры для снижения вероятности, воздействия или того и другого. Эти решения, как правило, включают выбор оптимального варианта из нескольких возможных.

Процесс SRM стремится обеспечить баланс между воздействием рисков и стоимостью решений в области безопасности, предназначенных для управления ими. При принятии решений способность мер в области безопасности спасать жизни, а также важность рассматриваемых программ и мандатов являются более важными факторами, чем объемы расходов.

Примечание для руководителей. Не основывайте свои решения на уровне угрозы. Принимайте решение о действиях после определения уровня уязвимости вашей организации к угрозам. Управление рисками учитывает как расходы, так и выгоды: оцените и то, и другое. Также важно учитывать расходы, связанные с отсутствием управления рисками: они могут быть неприемлемо высокими, поскольку нежелательные события не только оказывают первичное воздействие, но и становятся причиной вторичных и третичных издержек для организации, которую они затрагивают.

Не забывайте, что управление рисками также позволяет сэкономить средства за счет сокращения ущерба. При выборе возможных мер SRM важно учитывать:

- Что выявленная мера фактически снижает риск опасного события;
- Неблагоприятные воздействия. Попытки управлять одним риском могут непреднамеренно создать или увеличить другой риск. Например, длительный контроль доступа, который увеличивает время, необходимое, чтобы войти в помещение, может подвергнуть персонал угрозе, для смягчения которой и были разработаны меры контроля.
- Расходы. Устранение ущерба, причиненного угрозами, может оказаться дорогостоящим, однако и повышенные меры безопасности могут потребовать значительных средств.
- Дополнительные ресурсы. В том числе расходы на обучение, поддержку, техническое обслуживание и другие факторы, необходимые для обеспечения эффективности мер SRM.
- Время, необходимое для осуществления. В ситуациях, где временные ограничения

играют важную роль, необходимо рассмотреть несколько вариантов. В ходе принятия мер, вероятно, потребуются также промежуточные меры, которые позволят заполнить пробелы.

Комплексный подход, сочетающий в себе физические, процедурные, технические и людские аспекты, может многократно увеличить выгоду от мер SRM. Основанный на принципах сдерживания, обнаружения, задержки и исключения, такой подход часто называют концентрической многоуровневой безопасностью или эшелонированной обороной. В случае многоуровневой системы безопасности ее труднее преодолеть.

Процесс SRM достаточно гибок, чтобы гарантировать, что меры могут быть адаптированы к конкретной области SRM (если она отличается от заранее определенной области). Эта особенность устраняет необходимость принятия одинаковых минимальных мер по всей стране. Однако при этом необходимо выполнять требования, обязательные для всех мест службы, такие как обучение BSafe и стартовые наборы для профилактического лечения после воздействия (комплекты PEP). Примечание о включении подхода, ориентированного на отдельных лиц, в управление рисками безопасности

Обязательной является ориентация мер SRM на отдельных лиц. Ожидается, что специалисты в области безопасности будут взаимодействовать с группой по вопросам безопасности для определения подходящих, целесообразных и оперативных мер, которые помогут всему персоналу снизить риск до приемлемого уровня. В Руководстве по гендерным вопросам и «Учете инвалидности при управлении безопасностью» подробно изложены соображения, которые следует учитывать при определении мер по обеспечению РСА. Некоторые соображения включают, помимо прочего:

1. Меры, непосредственно связанные с выявленными описаниями событий и снижающие вероятность и/или воздействие события.
2. Меры, поддерживающие определенные категории персонала с различными профилями. Например, персонал UNSMS из другого региона/сообщества, религиозные меньшинства, женщины, представители ЛГБТИК+, люди с инвалидностью, беременные женщины и т. д.
3. Предлагаемые меры не должны налагать дискриминационных ограничений на персонал по признаку гендера, сексуальной ориентации, половых характеристик, идентичности и самовыражения.

УВКБ ООН обязано обеспечить выполнение положений, приведенных на стр. 22 Руководства «Гендерные вопросы в управлении безопасностью» и на стр. 6–10 отдельной главы «Учет инвалидности в управлении безопасностью».

Этап 7. Осуществление SRM

После определения мер безопасности и их согласования необходимо принять твердое обязательство по их безотлагательному осуществлению. Когда меры и процессы управления рисками одобрены на соответствующем уровне, они становятся обязательными. Следует разработать план осуществления, обеспечивающий

своевременное и эффективное принятие и завершение мер. Без этого этапа весь процесс SRM может потерпеть неудачу.

По этой причине руководители должны убедиться, что субъекты безопасности и другие соответствующие заинтересованные стороны (включая инженеров, ИКТ, отдел материально-технического снабжения, административный персонал и т. д.) применяют комплексный подход к управлению проектами, когда они подготавливают документацию по ресурсам планирования, организации и управления, необходимые для успешного осуществления мер SRM.

Необходимо учитывать следующие аспекты:

- Меры по предотвращению/смягчению последствий. Подготовьте подробный и точный список предлагаемых мер.
- Цели предотвращения/смягчения последствий. Объясните, как рассматриваемые меры позволят управлять выявленными рисками. Смогут ли они сделать это за счет снижения вероятности или воздействия, или того и другого?
- Ресурсы/расходы. Подробно опишите необходимые ресурсы, включая расходы на финансирование и сотрудничество. Учитывайте единовременные и периодические расходы (на техническое обслуживание, обучение и т. д.).
- Ответственные субъекты. Решите, кто из руководителей, физических или юридических лиц несет ответственность за осуществление каждой меры.
- Временные рамки. Определите реалистичный график осуществления каждой меры и срок, к которому проект должен быть завершен. Для устранения пробелов до полного осуществления основных мер могут потребоваться альтернативные или временные меры.
- Обновление информации о прогрессе. Регулярно подготавливайте новую информацию о ходе осуществления мер. Перечислите текущие и завершенные меры, а также необходимые дальнейшие шаги. Внедрите механизмы оценки, сбора доказательств и проверки.
- Бюджет. Определите, являются ли меры SRM совместными мерами нескольких учреждений системы ООН или мерами конкретного учреждения, чтобы определить соответствующего держателя бюджета и утверждение бюджетных ассигнований на запланированные меры.

Этап 8. Определение приемлемого уровня риска

Несмотря на то, что процесс SRM снижает уровень риска за счет смягчения и предотвращения (как описано в предыдущих разделах), не все риски можно устранить полностью. Приведенные ниже принципы предлагают UNSMS руководство в отношении определения приемлемого уровня риска.

- Не принимайте ненужный риск. Нет никакой пользы в принятии риска, если он не поможет ООН достичь своих целей.
- Принимайте риск, когда выгоды превышают потенциальные потери. Несмотря на то, что все риски устранить невозможно, попытка избежать любых рисков не поможет

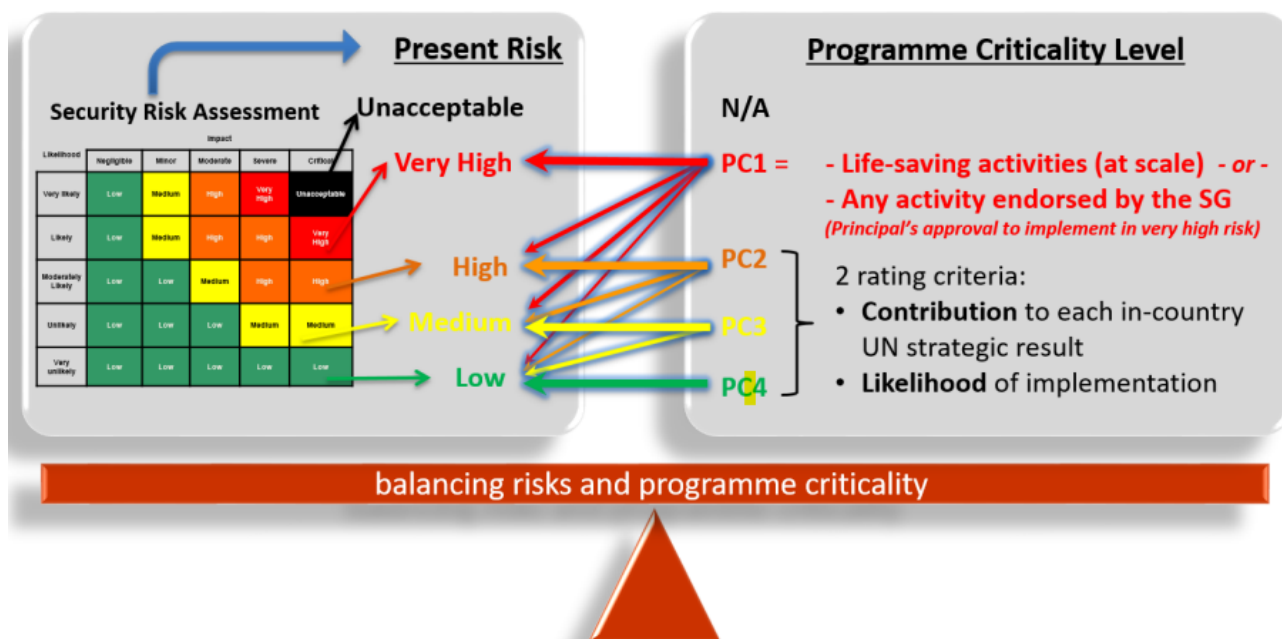
ООН достичь своих целей.

- Принимайте решения по управлению рисками на должном уровне. Организации должны обеспечить принятие решений о рисках на уровне высшего руководства. Руководители и персонал не должны принимать риск, который не был соответствующим образом одобрен.
- Следует принять все разумные меры для снижения риска. Мы всегда должны стараться снизить риск, когда это возможно, даже если определенная степень риска считается приемлемой.

Модель приемлемого уровня риска

Модель приемлемого уровня риска UNSMS обеспечивает баланс между рисками в области безопасности и преимуществами программы (так называемая «[критичность программы](#)»). Для оценки приемлемого уровня риска четыре уровня [критичности программы](#) (КП) сравниваются с уровнями риска, полученными на этапе 5 выше (SRA). Модель приемлемого уровня риска различает деятельность, осуществляемую персоналом ООН, и деятельность, осуществляемую партнерами-исполнителями, и касается только деятельности, осуществляемой персоналом ООН. Она устанавливает максимальный уровень риска безопасности, приемлемый для каждого уровня [критичности программы](#). Для установления уровней КП для деятельности с участием персонала ООН используется отдельный инструмент определения [критичности программы](#).

Существует уровень риска (самый высокий уровень вероятности и самый высокий уровень воздействия), который является неприемлемым, независимо от важности мероприятия, которое персонал ООН может стремиться осуществить. В таблице ниже представлена связь между приемлемым уровнем риска и ответственностью за принятие решений. (Предполагается, что организация сделала все возможное для снижения рисков безопасности.)



PC1 activities only in very high present risk environments;

PC1 - PC2 in high present risk environments;

PC1 - PC2 - PC3 in medium present risk environments;

PC1 - PC2 - PC3 - PC4 in low present risk environments.

Этап 9. Мониторинг и обзор

Целью мониторинга и оценки является повышение мер по управлению рисками безопасности и обеспечение больших возможностей осуществления программ с приемлемым уровнем риска. Мониторинг дает представление о прогрессе или его отсутствии в осуществлении мер SRM. Этот процесс часто называют «соответствием». Обзоры являются ключевым фактором обеспечения соответствия SRM поставленной цели.

Контрольный список

- Соберите информацию о структуре безопасности ООН и ключевых участниках (DO, ASC, SMT/ASMT), а также специалистах по вопросам безопасности УВКБ ООН, которые играют ключевую роль в осуществлении процесса SRM.
- Активно поддерживайте завершение всех этапов SRM. Обеспечьте учет и продвижение PCA в процессах SRM, чтобы гарантировать, что уровень любого

риска для УВКБ ООН является приемлемым для всех участников деятельности.

- Подготовьте анализ критичности программы совместно с другими организациями ООН и используйте информацию для поддержки планирования операций.
- Убедитесь, что риски, выявленные в рамках SRM, также отражены в собственном реестре рисков учреждения, а управление рисками соответствует мерам SRM.

4. Политика и руководящие принципы

5. Ссылки

[Руководство по политике безопасности – Система обеспечения безопасности ООН](#)
[Управление рисками: обязанность проявлять должную заботу, охрана труда, защита ...](#)

6. Основные контактные данные

Служба полевой безопасности УВКБ ООН (FSS), Отдел чрезвычайных ситуаций, снабжения и безопасности (ОЧСБС). По адресу: FS00@unhcr.org