

Подготовлено совместно
МАГАТЭ и МОУП-Интерполом

Риск-ориентированный подход к мерам физической ядерной безопасности ядерного и другого радиоактивного материала, находящегося вне регулирующего контроля

ПОДГОТОВЛЕНО СОВМЕСТНО
IAEA, ICPO-INTERPOL



IAEA



INTERPOL



IAEA

Международное агентство по атомной энергии

СЕРИЯ ИЗДАНИЙ МАГАТЭ ПО ФИЗИЧЕСКОЙ ЯДЕРНОЙ БЕЗОПАСНОСТИ

В Серии изданий МАГАТЭ по физической ядерной безопасности освещаются вопросы физической ядерной безопасности, касающиеся предупреждения и обнаружения преступных или преднамеренных несанкционированных действий, которые совершаются в отношении ядерного материала, другого радиоактивного материала, соответствующих установок или соответствующей деятельности, а также реагирования на подобные действия. Эти публикации соответствуют положениям международно-правовых документов по физической ядерной безопасности, таких как Конвенция о физической защите ядерного материала и поправка к ней, Международная конвенция о борьбе с актами ядерного терроризма, резолюции 1373 и 1540 Совета Безопасности Организации Объединенных Наций и Кодекс поведения по обеспечению безопасности и сохранности радиоактивных источников, и служат дополнением к ним.

КАТЕГОРИИ ПУБЛИКАЦИЙ В СЕРИИ ИЗДАНИЙ МАГАТЭ ПО ФИЗИЧЕСКОЙ ЯДЕРНОЙ БЕЗОПАСНОСТИ

Публикации Серии изданий МАГАТЭ по физической ядерной безопасности выпускаются в следующих категориях:

- **«Основы физической ядерной безопасности»** — в них формулируется цель государственного режима физической ядерной безопасности и описываются основные элементы такого режима. Они служат основой для рекомендаций по физической ядерной безопасности;
- **«Рекомендации по физической ядерной безопасности»** — в них излагаются меры, которые следует принимать государствам для создания и обеспечения функционирования эффективного национального режима физической ядерной безопасности в соответствии с «Основами физической ядерной безопасности»;
- **«Практические руководства»** — в них даются руководящие указания относительно средств, при помощи которых государства могли бы осуществлять меры, изложенные в рекомендациях по физической ядерной безопасности. По существу, в них рассматриваются пути выполнения рекомендаций, касающихся общих направлений деятельности в сфере физической ядерной безопасности;
- **«Технические руководящие материалы»** — в них в дополнение к указаниям, содержащимся в практических руководствах, даются руководящие указания по конкретным техническим вопросам. В них подробно разбирается порядок действий по осуществлению необходимых мер.

СОСТАВЛЕНИЕ И РЕЦЕНЗИРОВАНИЕ

В подготовке и рецензировании публикаций Серии изданий по физической ядерной безопасности участвуют Секретариат МАГАТЭ, эксперты из государств-членов (помогающие Секретариату в составлении публикаций) и Комитет по руководящим материалам по физической ядерной безопасности (КРМФЯБ), отвечающий за рецензирование и одобрение проектов публикаций. При необходимости в период работы над публикацией также проводятся технические совещания открытого состава, чтобы специалисты из государств-членов и соответствующих международных организаций могли рассмотреть и обсудить проект текста. Кроме того, для обеспечения международного рецензирования и достижения консенсуса на высоком уровне Секретариат представляет проекты текстов всем государствам-членам на официальное рассмотрение в течение 120-дневного срока.

Для каждой публикации Секретариат готовит следующие документы, которые поэтапно одобряются КРМФЯБ в процессе подготовки и рецензирования:

- набросок и план работы с описанием предполагаемой новой или пересмотренной публикации, ее предполагаемой цели, сферы применения и содержания;
- проект публикации для представления на отзыв государствам-членам в течение 120-дневного периода консультаций;
- окончательный проект публикации, в котором учтены замечания государств-членов.

В процессе подготовки и рецензирования публикаций Серии изданий МАГАТЭ по физической ядерной безопасности принимаются во внимание соображения конфиденциальности и учитывается тот факт, что вопросы физической ядерной безопасности неразрывно связаны с общими и конкретными интересами национальной безопасности.

Одним из основополагающих моментов является необходимость учета в техническом содержании публикаций соответствующих норм безопасности МАГАТЭ и деятельности по гарантиям. В частности, публикации Серии изданий по физической ядерной безопасности, посвященные вопросам, которые пересекаются с вопросами безопасности, — известные как документы по взаимосвязанной тематике — на каждом из вышеуказанных этапов рецензируются соответствующими комитетами по нормам безопасности, а также КРМФЯБ.

РИСК-ОРИЕНТИРОВАННЫЙ ПОДХОД К МЕРАМ
ФИЗИЧЕСКОЙ ЯДЕРНОЙ БЕЗОПАСНОСТИ
ЯДЕРНОГО И ДРУГОГО РАДИОАКТИВНОГО
МАТЕРИАЛА, НАХОДЯЩЕГОСЯ
ВНЕ РЕГУЛИРУЮЩЕГО КОНТРОЛЯ

Членами Международного агентства по атомной энергии являются следующие государства:

АВСТРАЛИЯ	ЙЕМЕН	ПОЛЬША
АВСТРИЯ	КАБО-ВЕРДЕ	ПОРТУГАЛИЯ
АЗЕРБАЙДЖАН	КАЗАХСТАН	РЕСПУБЛИКА МОЛДОВА
АЛБАНИЯ	КАМБОДЖА	РОССИЙСКАЯ ФЕДЕРАЦИЯ
АЛЖИР	КАМЕРУН	РУАНДА
АНГОЛА	КАНАДА	РУМЫНИЯ
АНТИГУА И БАРБУДА	КАТАР	САЛЬВАДОР
АРГЕНТИНА	КЕНИЯ	САМОА
АРМЕНИЯ	КИПР	САН-МАРИНО
АФГАНИСТАН	КИТАЙ	САУДОВСКАЯ АРАВИЯ
БАГАМСКИЕ ОСТРОВА	КОЛУМБИЯ	СВЯТОЙ ПРЕСТОЛ
БАНГЛАДЕШ	КОМОРСКИЕ ОСТРОВА	СЕВЕРНАЯ МАКЕДОНИЯ
БАРБАДОС	КОНГО	СЕЙШЕЛЬСКИЕ ОСТРОВА
БАХРЕЙН	КОРЕЯ, РЕСПУБЛИКА	СЕНЕГАЛ
БЕЛАРУСЬ	КОСТА-РИКА	СЕНТ-ВИНСЕНТ И ГРЕНАДИНЫ
БЕЛИЗ	КОТ-Д'ИВУАР	СЕНТ-КИТС И НЕВИС
БЕЛЬГИЯ	КУБА	СЕНТ-ЛЮСИЯ
БЕНИН	КУВЕЙТ	СЕРБИЯ
БОЛГАРИЯ	КЫРГЫЗСТАН	СИНГАПУР
БОЛИВИЯ, МНОГОНАЦИОНАЛЬНОЕ ГОСУДАРСТВО	ЛАОССКАЯ НАРОДНО- ДЕМОКРАТИЧЕСКАЯ РЕСПУБЛИКА	СИРИЙСКАЯ АРАБСКАЯ РЕСПУБЛИКА
БОСНИЯ И ГЕРЦЕГОВИНА	ЛАТВИЯ	СЛОВАКИЯ
БОТСВАНА	ЛЕСОТО	СЛОВЕНИЯ
БРАЗИЛИЯ	ЛИБЕРИЯ	СОЕДИНЕННОЕ КОРОЛЕВСТВО ВЕЛИКОБРИТАНИИ И СЕВЕРНОЙ ИРЛАНДИИ
БРУНЕЙ-ДАРУССАЛАМ	ЛИВАН	СОЕДИНЕННЫЕ ШТАТЫ АМЕРИКИ
БУРКИНА-ФАСО	ЛИВИЯ	СУДАН
БУРУНДИ	ЛИТВА	СЬЕРРА-ЛЕОНЕ
ВАНУАТУ	ЛИХТЕНШТЕЙН	ТАДЖИКИСТАН
ВЕНЕСУЭЛА, БОЛИВАРИАНСКАЯ РЕСПУБЛИКА	ЛЮКСЕМБУРГ	ТАИЛАНД
ВЬЕТНАМ	МАВРИКИЙ	ТОГО
ГАБОН	МАВРИТАНИЯ	ТОНГА
ГАИТИ	МАДАГАСКАР	ТРИНИДАД И ТОБАГО
ГАЙАНА	МАЛАВИ	ТУНИС
ГАМБИЯ	МАЛАЙЗИЯ	ТУРКМЕНИСТАН
ГАНА	МАЛИ	ТУРЦИЯ
ГВАТЕМАЛА	МАЛЬТА	УГАНДА
ГВИНЕЯ	МАРОККО	УЗБЕКИСТАН
ГЕРМАНИЯ	МАРШАЛЛОВЫ ОСТРОВА	УКРАИНА
ГОНДУРАС	МЕКСИКА	УРУГВАЙ
ГРЕНАДА	МОЗАМБИК	ФИДЖИ
ГРЕЦИЯ	МОНАКО	ФИЛИППИНЫ
ГРУЗИЯ	МОНГОЛИЯ	ФИНЛЯНДИЯ
ДАНИЯ	МЬЯНМА	ФРАНЦИЯ
ДЕМОКРАТИЧЕСКАЯ РЕСПУБЛИКА КОНГО	НАМИБИЯ	ХОРВАТИЯ
ДЖИБУТИ	НЕПАЛ	ЦЕНТРАЛЬНОАФРИКАНСКАЯ РЕСПУБЛИКА
ДОМИНИКА	НИГЕР	ЧАД
ДОМИНИКАНСКАЯ РЕСПУБЛИКА	НИГЕРИЯ	ЧЕРНОГОРИЯ
ЕГИПЕТ	НИДЕРЛАНДЫ	ЧЕШСКАЯ РЕСПУБЛИКА
ЗАМБИЯ	НИКАРАГУА	ЧИЛИ
ЗИМБАБВЕ	НОВАЯ ЗЕЛАНДИЯ	ШВЕЙЦАРИЯ
ИЗРАИЛЬ	НОРВЕГИЯ	ШВЕЦИЯ
ИНДИЯ	ОБЪЕДИНЕННАЯ РЕСПУБЛИКА ТАНЗАНИЯ	ШРИ-ЛАНКА
ИНДОНЕЗИЯ	ОБЪЕДИНЕННЫЕ АРАБСКИЕ ЭМИРАТЫ	ЭКВАДОР
ИОРДАНИЯ	ОМАН	ЭРИТРЕЯ
ИРАК	ПАКИСТАН	ЭСВАТИНИ
ИРАН, ИСЛАМСКАЯ РЕСПУБЛИКА	ПАЛАУ	ЭСТОНИЯ
ИРЛАНДИЯ	ПАНАМА	ЭФИОПИЯ
ИСЛАНДИЯ	ПАПУА — НОВАЯ ГВИНЕЯ	ЮЖНАЯ АФРИКА
ИСПАНИЯ	ПАРАГВАЙ	ЯМАЙКА
ИТАЛИЯ	ПЕРУ	ЯПОНИЯ

Устав Агентства был утвержден 23 октября 1956 года на Конференции по выработке Устава МАГАТЭ, которая состоялась в Центральных учреждениях Организации Объединенных Наций в Нью-Йорке. Устав вступил в силу 29 июля 1957 года. Центральные учреждения Агентства находятся в Вене. Главной целью Агентства является достижение «более скорого и широкого использования атомной энергии для поддержания мира, здоровья и благосостояния во всем мире».

СЕРИЯ ИЗДАНИЙ МАГАТЭ ПО ФИЗИЧЕСКОЙ ЯДЕРНОЙ
БЕЗОПАСНОСТИ, № 24-G

РИСК-ОРИЕНТИРОВАННЫЙ
ПОДХОД К МЕРАМ ФИЗИЧЕСКОЙ
ЯДЕРНОЙ БЕЗОПАСНОСТИ
ЯДЕРНОГО И ДРУГОГО
РАДИОАКТИВНОГО МАТЕРИАЛА,
НАХОДЯЩЕГОСЯ ВНЕ
РЕГУЛИРУЮЩЕГО КОНТРОЛЯ

ПРАКТИЧЕСКОЕ РУКОВОДСТВО

ПОДГОТОВЛЕНО СОВМЕСТНО
МЕЖДУНАРОДНЫМ АГЕНТСТВОМ ПО АТОМНОЙ ЭНЕРГИИ
И МЕЖДУНАРОДНОЙ ОРГАНИЗАЦИЕЙ УГОЛОВНОЙ
ПОЛИЦИИ — ИНТЕРПОЛОМ

МЕЖДУНАРОДНОЕ АГЕНТСТВО ПО АТОМНОЙ ЭНЕРГИИ
ВЕНА, 2024 ГОД

УВЕДОМЛЕНИЕ ОБ АВТОРСКОМ ПРАВЕ

Все научные и технические публикации МАГАТЭ защищены положениями Всемирной конвенции об авторском праве, принятой в 1952 году (Берн) и пересмотренной в 1972 году (Париж). Впоследствии авторские права были распространены Всемирной организацией интеллектуальной собственности (Женева) также на интеллектуальную собственность в электронной и виртуальной форме. Для полного или частичного использования текстов, содержащихся в печатных или электронных публикациях МАГАТЭ, должно быть получено разрешение, которое обычно оформляется соглашениями типа роялти. Предложения о некоммерческом воспроизведении и переводе приветствуются и рассматриваются в каждом случае в отдельности. Вопросы следует направлять в Издательскую секцию МАГАТЭ по адресу:

Группа маркетинга и сбыта (Marketing and Sales Unit)
Издательская секция
Международное агентство по атомной энергии
Венский международный центр,
а/я 100,
А1400 Вена, Австрия
Факс: +43 1 26007 22529
Тел.: +43 1 2600 22417
Эл. почта: sales.publications@iaea.org
<https://www.iaea.org/ru/publikacii>

© МАГАТЭ, 2024

Отпечатано МАГАТЭ в Австрии

Февраль 2024 года

STI/PUB/1678

**РИСК-ОРИЕНТИРОВАННЫЙ ПОДХОД К МЕРАМ
ФИЗИЧЕСКОЙ ЯДЕРНОЙ БЕЗОПАСНОСТИ
ЯДЕРНОГО И ДРУГОГО РАДИОАКТИВНОГО
МАТЕРИАЛА, НАХОДЯЩЕГОСЯ
ВНЕ РЕГУЛИРУЮЩЕГО КОНТРОЛЯ
МАГАТЭ, ВЕНА 2024 ГОД**

STI/PUB/1678

ISBN 978-92-0-436123-0 (ПЕЧАТНЫЙ ФОРМАТ)

ISBN 978-92-0-436023-3 (ФОРМАТ PDF)

ISSN 2788-8959

ПРЕДИСЛОВИЕ

Согласно Уставу, главной целью МАГАТЭ является достижение «более скорого и широкого использования атомной энергии для поддержания мира, здоровья и благосостояния во всем мире». Наша работа заключается как в предотвращении распространения ядерного оружия, так и в обеспечении доступа к ядерным технологиям в мирных целях в таких областях, как здравоохранение и сельское хозяйство. Крайне важно обеспечить безопасное обращение со всеми ядерными и другими радиоактивными материалами и установками, на которых они находятся, и их надлежащую защиту от преступных или преднамеренных несанкционированных действий.

Ответственность за обеспечение физической ядерной безопасности возлагается на каждое государство в отдельности, однако созданию и поддержанию эффективных режимов физической ядерной безопасности в немалой степени способствует международное сотрудничество. Центральная роль, которую МАГАТЭ играет в содействии такому сотрудничеству и оказании помощи государствам, широко признана. Эта роль МАГАТЭ находит воплощение в многочисленном членском составе организации, ее уставном мандате, уникальном экспертном потенциале и многолетнем опыте в области предоставления технической помощи и подготовки специальных практических руководящих материалов для государств.

Начиная с 2006 года МАГАТЭ выпускает Серию изданий по физической ядерной безопасности, предназначенную для оказания помощи государствам в создании эффективных национальных режимов физической ядерной безопасности. Эти публикации дополняют положения международно-правовых документов по физической ядерной безопасности, таких как Конвенция о физической защите ядерного материала и поправка к ней, Международная конвенция о борьбе с актами ядерного терроризма, резолюции 1373 и 1540 Совета Безопасности Организации Объединенных Наций и Кодекс поведения по обеспечению безопасности и сохранности радиоактивных источников.

Разработка руководящих материалов осуществляется при активном участии экспертов из государств — членов МАГАТЭ, благодаря которому в этих материалах находит отражение консенсус в отношении надлежащей практики обеспечения физической ядерной безопасности. Комитет МАГАТЭ по руководящим материалам по физической ядерной безопасности, учрежденный в марте 2012 года и состоящий из представителей государств-членов, занимается рассмотрением и одобрением проектов публикаций Серии изданий по физической ядерной безопасности по мере их подготовки.

МАГАТЭ вместе со своими государствами-членами будет и далее продолжать деятельность, направленную на то, чтобы блага от мирного применения ядерных технологий были доступны для целей улучшения здоровья, повышения благосостояния и процветания людей во всем мире.

РЕДАКЦИОННОЕ ПРИМЕЧАНИЕ

Руководящие материалы, опубликованные в Серии изданий МАГАТЭ по физической ядерной безопасности, не являются обязывающими документами для государств, однако государства могут использовать эти руководящие материалы в качестве документов, помогающих им выполнять свои обязательства, вытекающие из международно-правовых документов, а также осуществлять свои обязанности по обеспечению физической ядерной безопасности внутри государства. В тексте руководящих материалов используется формулировка «следует», отражающая международную надлежащую практику и указывающая на международный консенсус в отношении необходимости принятия государствами рекомендуемых или эквивалентных альтернативных мер.

Термины из области физической безопасности должны пониматься так, как они определены в публикации, в которой они используются, или в руководящих материалах более высокого уровня, которые данная публикация дополняет. В остальных случаях слова и выражения употребляются в своем общепринятом значении.

Дополнение рассматривается в качестве неотъемлемой части публикации. Материал, содержащийся в дополнении, имеет тот же статус, что и основной текст. Приложения используются для включения в публикацию практических примеров, дополнительной информации или пояснений. Приложения не являются неотъемлемой частью основного текста.

Для обеспечения точности информации, содержащейся в настоящей публикации, были приложены большие усилия, однако ни МАГАТЭ, ни его государства-члены не несут ответственности за последствия, которые могут возникнуть в результате использования этой информации.

Использование тех или иных названий стран или территорий не является выражением какого-либо суждения со стороны издателя, в роли которого выступает МАГАТЭ, относительно правового статуса таких стран или территорий, их органов и учреждений, либо относительно делимитации их границ.

Упоминание названий конкретных компаний или продуктов (независимо от того, указаны они как зарегистрированные или нет) не подразумевает какого-либо намерения нарушить права собственности и не должно толковаться как одобрение или рекомендация со стороны МАГАТЭ.

СОДЕРЖАНИЕ

1.	ВВЕДЕНИЕ	1
	Общие сведения (1.1–1.5)	1
	Цель (1.6)	3
	Область применения (1.7–1.8)	3
	Структура (1.9–1.10)	4
2.	ОСНОВА ОЦЕНКИ УГРОЗЫ И РИСК-ОРИЕНТИРОВАННОГО ПОДХОДА (2.1–2.6).....	5
	Национальная политика и стратегия в области физической ядерной безопасности (2.7)	7
	Административно-правовая основа (2.8)	8
	Функции и обязанности (2.9–2.11)	8
	Координационный механизм (2.12)	9
	Международное сотрудничество (2.13–2.14)	10
3.	ИДЕНТИФИКАЦИЯ УГРОЗ ФИЗИЧЕСКОЙ ЯДЕРНОЙ БЕЗОПАСНОСТИ (3.1–3.5)	11
	Уязвимость ядерного и другого радиоактивного материала, находящегося вне регулирующего контроля (3.6–3.9)	15
	Доступность ядерного и другого радиоактивного материала, находящегося вне регулирующего контроля (3.10–3.13)	16
	Трансграничные перемещения (3.14–3.17)	18
	Анализ возможностей и намерений злоумышленника (3.18–3.23)	19
4.	ИДЕНТИФИКАЦИЯ ЦЕЛЕЙ И ОЦЕНКА ПОТЕНЦИАЛЬНЫХ ПОСЛЕДСТВИЙ (4.1–4.2)	22
	Идентификация целей (4.3–4.6)	23
	Последствия событий, связанных с физической ядерной безопасностью (4.7–4.18)	25
5.	МЕТОДИКИ ОЦЕНКИ УГРОЗ И РИСКОВ (5.1–5.4)	30
	Методики оценки угроз (5.5–5.15)	32
	Методики оценки рисков (5.16–5.33)	39

6.	ПРИМЕНЕНИЕ РИСК-ОРИЕНТИРОВАННОГО ПОДХОДА (6.1–6.5)	49
	Создание условий (6.6)	50
	Оценка угроз и рисков (6.7)	51
	Определение альтернативных систем и мер физической ядерной безопасности (6.8–6.14)	51
	Внедрение систем и мер физической ядерной безопасности (6.15–6.17)	53
	Менеджмент рисков (6.18–6.22)	54
ПРИЛОЖЕНИЕ I.	БЛОК-СХЕМА ОЦЕНКИ УГРОЗ И ПРИМЕНЕНИЯ РИСК-ОРИЕНТИРОВАННОГО ПОДХОДА	57
ПРИЛОЖЕНИЕ II.	ПРИМЕР ОЦЕНКИ УГРОЗЫ	59
ПРИЛОЖЕНИЕ III.	ПРИМЕР ОЦЕНКИ РИСКА	68
ПРИЛОЖЕНИЕ IV.	ПРИМЕР ПРИМЕНЕНИЯ РИСК-ОРИЕНТИРОВАННОГО ПОДХОДА	74
	СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ	79
	ГЛОССАРИЙ	81

1. ВВЕДЕНИЕ

ОБЩИЕ СВЕДЕНИЯ

1.1. Обеспечение физической ядерной безопасности предполагает принятие мер по предупреждению преступных или преднамеренных несанкционированных действий в отношении ядерного материала, другого радиоактивного материала, связанных с ними установок или связанной с ними деятельности, обнаружению таких действий и реагированию на них. Следует применять надлежащий подход и в отношении других действий, которые, по определению государства, могут отрицательно влиять на физическую ядерную безопасность. Угроза ядерного терроризма вызывает обеспокоенность у всех государств, а риск использования ядерного или другого радиоактивного материала для совершения преступного действия¹ несет в себе серьезную угрозу национальной и международной безопасности с потенциально серьезными последствиями для людей, имущества и окружающей среды.

1.2. В настоящем практическом руководстве описываются концепции и методики применения риск-ориентированного подхода к физической ядерной безопасности ядерного и другого радиоактивного материала, находящегося вне регулирующего контроля², включая проведение оценок угроз³ и рисков, которые могут затем использоваться как источник информации при разработке и внедрении систем и мер физической ядерной безопасности. При подготовке настоящей публикации были использованы как национальный опыт, так и практические и руководящие публикации по

¹ Конвенция о физической защите ядерного материала и поправка к ней (статья 7) [1] и Международная конвенция о борьбе с актами ядерного терроризма (статья 2) [2] требуют от государств-участников сделать наказуемыми все преступления, которые имеют серьезные последствия для людей, имущества и окружающей среды.

² Термин «находящийся вне регулирующего контроля» означает отсутствие надлежащего официального разрешения на ядерный материал или другой радиоактивный материал — либо в результате утраты контроля по той или иной причине, либо вследствие его изначального отсутствия.

³ В данной публикации конкретный термин «угроза физической ядерной безопасности» используется в том значении, в каком он определен в «Основах физической ядерной безопасности» [3]. Термин «угроза» без уточнений используется в более общем смысле для обозначения представляющего угрозу субъекта (также называемого злоумышленником) либо представляющего угрозу объекта (также называемого устройством).

физической ядерной безопасности, оценке угроз и менеджменте рисков. Настоящая публикация дополняет издание категории «Основы физической ядерной безопасности» [3] и согласуется со следующими рекомендациями по физической ядерной безопасности:

- «Рекомендации по физической ядерной безопасности, касающиеся физической защиты ядерных материалов и ядерных установок (INFCIRC/225/Revision 5)» [4];
- «Рекомендации по физической ядерной безопасности, касающиеся радиоактивных материалов и связанных с ним установок» [5];
- «Рекомендации по физической ядерной безопасности, касающиеся ядерных и других радиоактивных материалов, находящихся вне регулирующего контроля» [6].

1.3. В контексте настоящего практического руководства «риск» — это возможность нежелательного исхода какого-либо события, связанного с физической ядерной безопасностью, определяемая его вероятностью и соответствующими последствиями, если таковые наступят, включая последствия для людей, имущества и окружающей среды. Вообще говоря, риск представляет собой производную от трех компонентов: угрозы, уязвимости и последствий. Необходимым условием для определения приоритетов и разработки надлежащих систем и мер физической ядерной безопасности является применение риск-ориентированного подхода [6]. Оценки угроз и рисков позволяют государствам управлять рисками и устанавливать приоритеты при распределении ресурсов (например, людских и финансовых) между организациями и системами и мерами физической ядерной безопасности.

1.4. Риск-ориентированный подход представляет собой итеративный процесс идентификации и оценки угроз и рисков, разработки, оценки и внедрения альтернативных систем и мер, а также проверки разработанных мер на релевантность и эффективность и управления такими мерами. Настоящая публикация уделяет особое внимание оценке угроз и рисков как элементу риск-ориентированного подхода⁴, соответствующего международным рекомендациям [7]. Риск-ориентированный подход может помочь государству более эффективно и рационально распределять свои ресурсы за счет систематического учета угроз и рисков.

⁴ Термин «риск-ориентированный подход» в основном относится к тому же циклическому процессу управления рисками, который охватывается понятием «менеджмент риска».

1.5. Настоящее практическое руководство дополняет руководство по разработке, использованию и актуализации проектной угрозы в отношении ядерного материала, другого радиоактивного материала, соответствующих установок и соответствующей деятельности [8]. Дополнительную информацию об угрозах, а также техническую информацию о мерах физической ядерной безопасности можно найти во вспомогательном руководстве по борьбе с незаконным оборотом ядерного материала и другого радиоактивного материала [9].

ЦЕЛЬ

1.6. Цель настоящей публикации — дать государствам руководство по разработке риск-ориентированного подхода и проведению оценок угроз и рисков как основу для проектирования и внедрения устойчивых систем и мер физической ядерной безопасности в целях предупреждения преступных или преднамеренных несанкционированных действий с ядерным и другим радиоактивным материалом, находящимся вне регулирующего контроля, обнаружения таких действий и реагирования на них. Настоящая публикация призвана стать руководством для директивных органов, правоохранительных структур и экспертов из компетентных органов и других профильных организаций.

ОБЛАСТЬ ПРИМЕНЕНИЯ

1.7. Настоящая публикация посвящена рассмотрению риск-ориентированного подхода и методологий оценки угроз и рисков в целях разработки систем и мер физической ядерной безопасности ядерного или другого радиоактивного материала, о котором известно, что он находится вне регулирующего контроля, а также оставленного, утерянного, пропавшего или похищенного материала, о котором не было известно, что он является таковым, или же который был обнаружен каким-либо иным способом.

1.8. Настоящая публикация не охватывает оценку угроз и рисков для ядерного материала, другого радиоактивного материала, соответствующих установок или соответствующей деятельности, которые находятся под регулирующим контролем. Тем не менее в ней учитывается потенциальная возможность утери, пропажи или хищения материала. Руководящие указания по оценке угрозы хищения таких материалов и саботажа

(диверсии) на таких установках можно найти в документах Серии изданий МАГАТЭ по физической ядерной безопасности (см. [4, 5, 8, 10]). Настоящая публикация не касается вопросов проектирования и внедрения систем и мер обнаружения событий, связанных с физической ядерной безопасностью, и реагирования на них (см. [11, 12]).

СТРУКТУРА

1.9. В разделе 2, следующем за введением, описываются основополагающие принципы менеджмента рисков, связанных с ядерным и другим радиоактивным материалом, находящимся вне регулирующего контроля, и, в частности, роли и обязанности, административно-правовая основа проведения оценок угроз и рисков, а также механизмы координации указанной деятельности на национальном и международном уровнях. В разделе 3 даются руководящие указания по идентификации угроз физической ядерной безопасности. В нем описываются источники угроз («угрозы, исходящие от...») и пути их происхождения. Раздел 4 охватывает методы и процедуры идентификации целей («угрозы для...») и оценку потенциальных последствий. В разделе 5 разбираются методики оценки угроз и рисков и оценки вероятности возникновения угроз. Раздел 6 содержит общее описание того, каким образом риск-ориентированный подход, включающий использование оценки угроз и рисков, способствует определению альтернативных мер, внедрению систем и мер физической ядерной безопасности и управлению ими.

1.10. В приложениях I–IV, следующих за основным текстом, представлены гипотетические, воображаемые оценки угроз и рисков в качестве примера применения риск-ориентированных подходов. Эти приложения взаимосвязаны и в своей совокупности дают полную картину риск-ориентированного подхода. В приложении I представлена полная блок-схема риск-ориентированного подхода, включая действия по оценке угроз и рисков. В приложении II содержатся примеры оценки угроз при помощи двух методик: подхода, основанного на описании угроз, и подхода, основанного на ранжировании угроз. В приложении III представлен пример подхода к оценке риска методом вероятностной оценки рисков. В приложении IV содержится пример риск-ориентированного подхода, основанного на использовании результатов оценки угроз и рисков для оценки и определения приоритетности действий по

разработке и внедрению систем и мер физической ядерной безопасности. В приложениях II–IV в качестве примера используется типичное государство, именуемое «условным государством».

2. ОСНОВА ОЦЕНКИ УГРОЗЫ И РИСК-ОРИЕНТИРОВАННОГО ПОДХОДА

2.1. Во всем мире радиоактивные источники, ядерные и другие радиоактивные материалы массово используются в таких сферах, как научные исследования, здравоохранение, сельское хозяйство, образование и промышленность. Если такие материалы находятся или оказываются вне регулирующего контроля, возникает потенциальная возможность их использования в преступных или преднамеренных несанкционированных действиях. Потенциальные последствия преступного или преднамеренного несанкционированного действия с ядерным и другим радиоактивным материалом, находящимся вне регулирующего контроля, зависят от количества материала, его формы, состава и активности. Использование такого материала со взрывчатой ​​веществом для создания «устройства»⁵ может увеличить потенциальный эффект от преступного или преднамеренного несанкционированного действия с ядерным материалом или другим радиоактивным материалом, особенно в случаях применения на стратегическом объекте. Такие действия могут привести к серьезным социальным, психологическим и экономическим последствиям, нанести ущерб здоровью и имуществу, а также повлечь за собой политические и экологические последствия. Это могут быть следующие действия:

- a) намеренное рассеивание радиоактивного материала в общественном месте, например с помощью радиологического диспергирующего устройства (РДУ);
- b) размещение радиоактивного материала в общественном месте, например в виде радиационного облучающего устройства (РОУ), с намерением облучить людей, находящихся вблизи от него;
- c) производство ядерного взрыва с помощью самодельного ядерного устройства (СЯУ).

⁵ Термин «устройство» в данной публикации используется для обозначения РДУ, РОУ и СЯУ. Это также соответствует определению, данному в Международной конвенции о борьбе с актами ядерного терроризма [2].

2.2. Как указывается в соответствующей публикации категории рекомендаций по физической ядерной безопасности [6], для учета существующих угроз проектирование систем и мер физической ядерной безопасности ядерного и другого радиоактивного материала, находящегося вне регулирующего контроля, должно состоять из четырех этапов:

- идентификация угроз;
- идентификация и оценка целей и последствий;
- оценка угроз и рисков;
- использование риск-ориентированного подхода при определении приоритетности систем и мер физической ядерной безопасности.

2.3. В процессе идентификации угроз следует учитывать потенциальных злоумышленников, которые могут запланировать использование ядерного материала или другого радиоактивного материала в преступном или преднамеренном несанкционированном действии для достижения собственных целей, а также потенциальную доступность для таких лиц или организаций как внутри, так и за пределами государства ядерного или другого радиоактивного материала, пригодного для совершения такого действия.

2.4. При идентификации и оценке потенциальных целей того или иного действия с ядерным или другим радиоактивным материалом, находящимся вне регулирующего контроля, должна учитываться привлекательность данной цели для злоумышленника. Такая привлекательность может быть обусловлена уязвимостью цели для данного действия или потенциальными последствиями действия, направленного на эту цель.

2.5. При оценке угроз следует учитывать мотив, намерения и возможности тех лиц или групп, которые, как предполагается на основе анализа полученных данных и информации, могут совершить преступное или преднамеренное несанкционированное действие. При оценке угроз следует учитывать такие факторы, как оценка потенциальной доступности ядерного или другого радиоактивного материала для таких лиц и опыт известных инцидентов, связанных с материалом, находящимся вне регулирующего контроля. Чтобы оценка была полной, она может охватывать информацию, полученную от контртеррористических и правоохранительных органов, а также от всех ведомств, участвующих в обеспечении ядерной и физической безопасности ядерного материала, другого радиоактивного материала, соответствующих установок и соответствующей деятельности. При оценке

угрозы следует также принимать во внимание техническую возможность и исторические обстоятельства использования такого материала в преступных или преднамеренных несанкционированных действиях.

2.6. При оценке риска учитывается вероятность совершения действия в сочетании с вероятностью успеха и уровнем последствий, что может быть использовано для определения приоритетности внедряемых систем и мер физической ядерной безопасности. Процесс учета информации о рисках при определении приоритетности систем и мер физической ядерной безопасности, а также в общем управлении системами физической ядерной безопасности называется риск-ориентированным подходом. Наилучшие методы менеджмента рисков определяются международными отраслевыми стандартами [7]. В рамках настоящего практического руководства указанные методы адаптированы для нужд разработки и определения приоритетности систем и мер физической ядерной безопасности.

НАЦИОНАЛЬНАЯ ПОЛИТИКА И СТРАТЕГИЯ В ОБЛАСТИ ФИЗИЧЕСКОЙ ЯДЕРНОЙ БЕЗОПАСНОСТИ

2.7. Эффективные системы и меры физической ядерной безопасности ядерного и другого радиоактивного материала, находящегося вне регулирующего контроля, должны иметь в своей основе всеобъемлющую и комплексную национальную политику и стратегию в области физической ядерной безопасности. Национальная политика и стратегия в области физической ядерной безопасности должна базироваться на национальных оценках угроз и рисков, и в ней должен быть определен компетентный орган, ответственный за проведение национальных оценок угроз и рисков физической ядерной безопасности и за взаимодействие и координацию усилий между всеми участвующими компетентными органами и организациями. Такая политика и стратегия должна определять объем и приоритетность превентивных мер, а также мер обнаружения и реагирования на события, связанные с физической ядерной безопасностью, на основе дифференцированного подхода. В нее также следует включать требование о периодической актуализации оценки угроз и рисков в свете меняющихся условий и новой информации, и ее следует пересматривать и актуализировать с учетом изменений, внесенных в оценку угроз и рисков. Проектирование систем и мер физической ядерной безопасности должно также базироваться на результатах оценки угроз и применении риск-ориентированного подхода [6].

АДМИНИСТРАТИВНО-ПРАВОВАЯ ОСНОВА

2.8. В целях разработки и реализации национальной политики и стратегии в области физической ядерной безопасности должна быть создана административно-правовая основа [6, 13]. Это особенно важно для распределения обязанностей между компетентными органами, а также для создания механизма взаимодействия и координации при проведении оценок угроз и рисков. В эту основу следует включить:

- a) требование о проведении оценок угроз и рисков и внедрении риск-ориентированных подходов;
- b) определение функций и обязанностей ответственного компетентного органа по проведению оценок угроз и рисков, связанных с ядерным и другим радиоактивным материалом, находящимся вне регулирующего контроля;
- c) возложение на соответствующий компетентный орган конкретной ответственности за разработку риск-ориентированного подхода и предоставление ему всех необходимых правовых и административных полномочий для осуществления такого процесса;
- d) положение о том, что все соответствующие компетентные органы должны оказывать всяческое содействие компетентному органу, ответственному за проведение оценок угроз и рисков, в деле внедрения систем и мер физической ядерной безопасности ядерного и другого радиоактивного материала, находящегося вне регулирующего контроля;
- e) положение о том, что компетентному органу, ответственному за проведение оценок угроз и рисков, следует по мере необходимости периодически актуализировать такую оценку;
- f) положение о том, что компетентным органам, ответственным за внедрение систем и мер физической ядерной безопасности, следует при проектировании таких систем и мер брать за основу результаты риск-ориентированного подхода.

ФУНКЦИИ И ОБЯЗАННОСТИ

2.9. Компетентному органу, ответственному за оценки угроз и рисков, связанных с ядерным и другим радиоактивным материалом, находящимся вне регулирующего контроля, следует иметь в наличии необходимые ресурсы и возможности для проведения оценок угроз и рисков во

взаимодействии с другими соответствующими компетентными органами, принимающими решения с учетом факторов риска в своих собственных зонах ответственности.

2.10. Уполномоченному компетентному органу следует обеспечить сбор и анализ всех соответствующих данных и проведение оценок угроз и рисков квалифицированным и компетентным персоналом. Результаты оценок должны быть изучены соответствующими компетентными органами в целях проектирования и определения приоритетности систем и мер физической ядерной безопасности. Всем соответствующим компетентным органам следует сотрудничать друг с другом на протяжении всего процесса оценки угроз и рисков, с тем чтобы результаты оценки отражали их точку зрения и дали им полезную информацию для применения собственного риск-ориентированного подхода.

2.11. Поскольку оценки угроз и рисков необходимо поддерживать в актуальном состоянии, всем соответствующим компетентным органам следует высказывать свои замечания и держать компетентный орган, ответственный за проведение оценок угроз и рисков, в курсе всех событий, связанных с физической ядерной безопасностью. Поскольку оценки угроз и рисков используются для определения приоритетности систем и мер физической ядерной безопасности, циклы оценок угроз и рисков могут быть увязаны с бюджетными или программными циклами с целью гарантировать доступ лиц, участвующих в принятии решений, к текущей информации и результатам.

КООРДИНАЦИОННЫЙ МЕХАНИЗМ

2.12. Проведение оценок угроз и рисков зависит от чувствительной информации, поступающей от ряда компетентных органов. Обмен достоверной и своевременной информацией, связанной с физической ядерной безопасностью, необходимо должным образом координировать на национальном и международном уровне в соответствии с политикой и правилами информационной безопасности, а также международными обязательствами. Механизмы такого информационного обмена следует базировать на утвержденных протоколах и процедурах передачи информации о событиях, имеющих последствия для физической ядерной безопасности, таких как утрата, пропажа или хищение ядерного материала и другого радиоактивного материала. Компетентному органу, ответственному за оценки угроз и рисков, следует информировать все другие соответствующие

компетентные органы о подготовке актуализированных оценок угроз и рисков в соответствии с принципом служебной необходимости. Тесное взаимодействие и координация имеют особенно важное значение в тех случаях, когда за оценку угроз и рисков отвечают несколько компетентных органов.

МЕЖДУНАРОДНОЕ СОТРУДНИЧЕСТВО

2.13. Эффективное участие в международной деятельности может стать источником информации и опыта, которые могут быть использованы для улучшения методов и процедур оценки угроз и рисков. Осведомленность о событиях, связанных с физической ядерной безопасностью, за пределами государства может также помочь лучше понять угрозу, существующую внутри государства. База данных МАГАТЭ по инцидентам и незаконному обороту (ITDB) является международной площадкой для сбора текущей информации о зарегистрированных случаях отсутствия регулирующего контроля над ядерным и другим радиоактивным материалом, а также о случаях его нахождения или обнаружения [14]. Анализ данных, представленных в ITDB, может дать представление о возможных угрозах или трансграничных перемещениях, которые могут нанести ущерб государству, и о возможных последствиях этого для оценки угроз и рисков. Такая информация может быть полезна государствам-членам при обсуждении оценок угроз и рисков.

2.14. Кроме того, участие в информационных и учебных семинарах, организуемых международными организациями и в рамках других двухсторонних и многосторонних инициатив, может использоваться для ознакомления персонала с новейшими методиками и процедурами и помочь в приобретении опыта и компетентности. Содействие в вопросах, связанных с оценкой угроз, может оказываться при посредничестве соответствующих международных организаций либо может запрашиваться напрямую на двухсторонней или многосторонней основе.

3. ИДЕНТИФИКАЦИЯ УГРОЗ ФИЗИЧЕСКОЙ ЯДЕРНОЙ БЕЗОПАСНОСТИ

3.1. Угрозы могут идентифицироваться как «угрозы, исходящие от...» и «угрозы для...». При идентификации «угроз, исходящих от...» учитывается личность злоумышленника, тип ядерного материала или другого радиоактивного материала, которым обладает злоумышленник или доступ к которому злоумышленник стремится получить, и возможный способ использования злоумышленником этого материала для причинения вреда. В контексте ядерного и другого радиоактивного материала, находящегося вне регулирующего контроля, которым может завладеть злоумышленник, вопрос о способе — это, как правило, вопрос о типе устройства, которое может попытаться использовать злоумышленник. При идентификации «угроз для...» учитываются стратегические объекты, против которых может использоваться ядерный или другой радиоактивный материал, находящийся вне регулирующего контроля. Конкретные составляющие, которые могут учитываться при оценке угроз, обобщены на рис. 1. При необходимости государства могут также учитывать дополнительные составляющие.

3.2. Составляющие, отвечающие на вопросы «КТО/ПОЧЕМУ», призваны идентифицировать и описать злоумышленников, которые могут попытаться совершить преступные или преднамеренные несанкционированные

КТО/ПОЧЕМУ (злоумышленник)	ЧТО (материал)	КАК/КОГДА/ГДЕ (тактика)
<ul style="list-style-type: none">• Намерение• Технические возможности• Финансовые возможности• Организационные возможности• Местоположение• Задачи• Наклонности• Установки	<ul style="list-style-type: none">• Тип и количество материала• Форма материала• Способ приобретения<ul style="list-style-type: none">• Хищение• Покупка• Случайность• Местонахождение материала	<ul style="list-style-type: none">• Конструкция устройства• Цель• Ожидаемый эффект• Маршрут перевозки• Сроки• Логистика• Возможность адаптации• Обман и шантаж

РИС. 1. Составляющие угроз.

действия. Следует провести анализ мотивов⁶, намерений и возможностей потенциальных злоумышленников. В него следует включать злоумышленников, которые могут попытаться совершить преступные или преднамеренные несанкционированные действия внутри государства, затрагивающие другое государство. Злоумышленников следует оценивать, исходя из вероятности совершения ими конкретных действий, их способности получить финансовые средства и технические возможности, необходимые для приобретения материала и изготовления устройства, а также владения ими информацией, необходимой для успешного осуществления данного действия. В пунктах 3.18–3.23 более подробно описаны методы и процессы анализа злоумышленников.

3.3. Составляющая анализа, отвечающая на вопрос «ЧТО», определяет материал, который может быть использован злоумышленником. При наличии в государстве небольшого числа мест, где хранится или используется ядерный материал и другой радиоактивный материал, соответствующие установки и соответствующая деятельность могут оцениваться по отдельности. В государстве с большим количеством установок и видов деятельности они могут оцениваться в составе однотипных групп или по отдельности — в зависимости от желаемого уровня детальности оценки. Помимо таких установок и видов деятельности, следует учитывать возможность приобретения материала за пределами государства или в результате его незаконного оборота. В круг возможных вариантов могут входить разные типы материала, которые могут быть приобретены, разные типы объектов, на которых хранится или используется материал, и методы, которые могут быть выбраны злоумышленником для приобретения материала или его контрабандного ввоза или вывоза из государства. Вероятность выбора конкретной установки или материала следует оценивать на основе знаний об общих предпочтениях злоумышленника, доступности материала или типа устройства, которое может быть выбрано злоумышленником. Вероятность приобретения материала зависит от возможностей злоумышленника и уязвимости материала. Часто для

⁶ Мотив может быть полезным фактором при выявлении потенциальных злоумышленников и типов преступных или других несанкционированных действий, которые они могут предпринять (например, мотивы злоумышленников могут повлиять на выбор ими целей). Однако несмотря на то, что принимаемые меры физической ядерной безопасности могут влиять на намерения и возможности злоумышленников, они не влияют на их мотивы. Таким образом, хотя мотивы и могут сыграть определенную роль при идентификации угроз, они могут быть не столь актуальными для других аспектов оценки угроз, а также для проектирования и внедрения систем и мер физической ядерной безопасности.

оценки вероятности приобретения материала злоумышленником могут использоваться данные имеющихся оценок уязвимости. В пунктах 3.6–3.9 говорится о том, как оценить возможность приобретения материала на соответствующих установках и в ходе соответствующей деятельности государства. В пунктах 3.10–3.17 описываются уязвимости, которые могут быть характерны для материала, находящегося вне регулирующего контроля внутри государства, и материала, пересекающего государственные границы.

3.4. Составляющие анализа, отвечающие на вопросы «КАК/КОГДА/ГДЕ», описывают характеристики конкретной тактики. Например, если предположить, что злоумышленник завладел материалом, то существуют два ключевых шага, которые ему, возможно, потребуется предпринять для изготовления устройства. Первый шаг — это приспособление материала к устройству или изменение его формы таким образом, чтобы его можно было использовать в устройстве. Второй шаг — это проектирование и конструирование самого устройства. Разные конструкции и разные уровни навыков изготовления устройств могут стать причиной создания устройств с разными уровнями эффективности. Для разработки более сложных конструкций может потребоваться больше времени, больше людей, а также более сложная инфраструктура (например, специальные инструменты или безопасное рабочее место), тогда как устройства менее сложной конструкции могут быть созданы быстрее и увереннее, без необходимости использования специального оборудования. Результатом анализа является оценка вероятности создания устройств разной степени эффективности — в зависимости от допущений, связанных с приобретаемым материалом и возможностями злоумышленника. Другие сценарии, такие как незаконный оборот, необязательно предполагают наличие устройства и могут рассматриваться как часть более крупного сценария действий злоумышленника с устройством либо как отдельное, самостоятельное действие. Готовое устройство обычно необходимо доставить к цели, в отношении которой оно будет применено. Поэтому необходимо учитывать как конечную цель (которая, в свою очередь, повлияет на уровень последствий), так и маршрут перевозки. Вероятность того, что злоумышленники будут перехвачены прежде, чем устройство будет пущено в ход, можно рассчитать, приняв во внимание возможности обнаружения с использованием средств сигнализации, информационных оповещений или других обычных правоохранительных действий и информации как части государственной архитектуры обнаружения событий, связанных с физической ядерной безопасностью [11]. Более подробное руководство по оценке составляющих «как», «когда» и «где» представлено в пунктах 4.3–4.6. При оценке применения устройства важно

учитывать его эффективность и потенциальные последствия. Последствия следует оценивать с точки зрения как предполагаемого эффекта, так и вероятного фактического эффекта. Более подробное руководство по оценке последствий какого-либо действия для физической ядерной безопасности представлено в пунктах 4.7–4.18.

3.5. Оценка угроз — это попытка охарактеризовать и, если возможно, количественно измерить угрозы посредством процесса идентификации или оценки злоумышленников или действий, которые могут причинить вред людям, имуществу, обществу или окружающей среде. Оценка угроз обычно основывается на оценке намерений и возможностей злоумышленников, где намерение часто выражается частотой (например, количеством попыток в год), а возможность — вероятностью успеха при попытке совершения действия. Ниже описаны три типичных подхода, которые также могут применяться в сочетании друг с другом.

- a) Степень угрозы может оцениваться качественно — просто как низкая, средняя или высокая (или по шкале, подобной той, которая приведена в таблице 1 раздела 4) — либо с помощью более сложных шкал, использующих качественные дескрипторы или критерии для ранжирования угроз, иногда именуемых «метаграммы». Эту простейшую форму качественной оценки угроз следует в обязательном порядке подкреплять экспертным заключением.
- b) Степень угрозы может оцениваться количественно на основе экспертного анализа и эмпирических данных. При использовании таких количественных оценок может быть очень сложно рассчитать значения вероятности, и поэтому при выполнении каждой оценки вероятности важно также оценивать степень ее неопределенности.
- c) Для нужд физической безопасности значения вероятности, связанные с угрозами, часто вообще не рассчитываются. Вместо этого меры физической безопасности оцениваются исходя из конкретного реального или гипотетического злоумышленника с определенными возможностями. Этот подход называется проектной угрозой (ПУ), поскольку выявленные возможности, по существу, определяют технические характеристики для проектирования систем и мер физической безопасности. Процесс разработки ПУ для ядерной установки описан в документе «Development, Use and Maintenance of the Design Basis Threat» («Разработка, использование и актуализация проектной угрозы») [8]. Аналогичный подход может использоваться

и для других нужд, связанных с физической ядерной безопасностью (например, для мер физической ядерной безопасности, принимаемых во время крупного общественного мероприятия).

УЯЗВИМОСТЬ ЯДЕРНОГО И ДРУГОГО РАДИОАКТИВНОГО МАТЕРИАЛА, НАХОДЯЩЕГОСЯ ВНЕ РЕГУЛИРУЮЩЕГО КОНТРОЛЯ

3.6. В целях совершения преступного или преднамеренного несанкционированного действия с ядерным материалом или другим радиоактивным материалом злоумышленник должен его приобрести⁷. Злоумышленник может попытаться приобрести материал на существующих установках и в ходе существующей деятельности, у других сторон, обладающих материалом, который уже находится вне регулирующего контроля, либо за пределами государства. В рамках оценки угроз важно оценить вероятность утраты регулирующего контроля над материалом, находящимся под таким контролем. В ITDB собрана информация со всего мира, которая показывает, что регулирующий контроль над материалами может быть утрачен либо отсутствовать в результате хищения, случайной потери или несанкционированной утилизации [14].

3.7. Одним из методов оценки вероятности того, что регулирующий контроль над материалом будет утрачен, является сравнение возможностей идентифицированных злоумышленников с уязвимостью соответствующих установок и соответствующей деятельности, в которой используется такой материал.

3.8. Операторы соответствующих установок или соответствующей деятельности, возможно, уже провели оценку уязвимости на основе ПУ или альтернативного заключения об угрозах и поэтому могут иметь представление об эффективности своих систем и мер физической ядерной безопасности в плане противодействия данной конкретной угрозе. ПУ следует определить таким образом, чтобы вероятность того, что

⁷ Как указано в пункте 1.9, настоящее практическое руководство применяется к ядерному и другому радиоактивному материалу, находящемуся вне регулирующего контроля, и поэтому преступные или преднамеренные несанкционированные действия, направленные против ядерного материала, другого радиоактивного материала, соответствующих установок и соответствующей деятельности (т.е. акты саботажа (диверсии)) данной публикацией не охватываются.

хорошо спроектированная система физической ядерной безопасности не удержит злоумышленника с возможностями, равными или меньшими по сравнению с теми, которые определены в ПУ, от успешного изъятия материала, была крайне мала. Однако уязвимость следует оценивать для всех соответствующих установок и видов деятельности, часть которых, возможно, не проводили собственных оценок уязвимости. Кроме того, если идентифицируются злоумышленники с возможностями, превышающими или качественно отличающимися от тех, которые определены в ПУ, для оценки вероятности успеха такого злоумышленника могут потребоваться дополнительные расчеты, аналогичные тем, которые выполняются для разработки ПУ. Следует рассмотреть несколько альтернативных методов незаконного приобретения материалов с установки или в процессе деятельности (в том числе во время перевозки), таких как вооруженное нападение, кража, пособничество инсайдера, подделка документов по учету материалов и хищение.

3.9. Злоумышленники, скорее всего, будут выбирать те установки или виды деятельности, где материалы наиболее уязвимы. Таким образом, вероятность приобретения злоумышленником материала может быть приблизительно равна вероятности приобретения материала с наиболее уязвимого объекта. Аналогичным образом, вероятность выбора злоумышленником конкретной установки или маршрута перевозки для приобретения материала связана с уязвимостью данной установки или маршрута перевозки. Более уязвимые объекты будут выбраны с большей вероятностью. Таким образом, изменение уязвимости любого объекта также ведет к изменению угрозы. Это имеет значение для анализа альтернативных вариантов. Когда в системы и меры физической ядерной безопасности на том или ином объекте вносятся изменения, может измениться степень уязвимости материала на этом объекте, что может также привести к потенциальному изменению как величины угрозы, так и наиболее вероятных сценариев ее реализации.

ДОСТУПНОСТЬ ЯДЕРНОГО И ДРУГОГО РАДИОАКТИВНОГО МАТЕРИАЛА, НАХОДЯЩЕГОСЯ ВНЕ РЕГУЛИРУЮЩЕГО КОНТРОЛЯ

3.10. Злоумышленники также могут искать возможности для приобретения ядерного и другого радиоактивного материала, который уже находится вне регулирующего контроля. Радиоактивные материалы имеются практически во всех странах, и их сохранность обеспечивается на разных уровнях. Некоторые ядерные материалы могут быть не учтены должным образом,

а некоторые радиоактивные источники могут не иметь надлежащей регистрации [5]. Некоторые оставленные, потерянные, пропавшие или похищенные ядерные и другие радиоактивные материалы могут не фиксироваться в отчетности как находящиеся вне регулирующего контроля.

3.11. С 1993 по конец 2012 года в ITDB поступило более 2000 сообщений о случаях утраты регулирующего контроля над ядерным и другим радиоактивным материалом [14]. Сообщения о материалах, находящихся вне регулирующего контроля, следует учитывать при оценке угроз. Сообщалось о лицах, незаконным образом предлагавших на продажу ядерный материал и другой радиоактивный материал, а также о лицах, пытавшихся приобрести ядерный материал и другой радиоактивный материал — по-видимому, для использования в преступных целях. Хотя многие предложения о поставке такого материала оказались мошенническими, могут иметь место необнаруженные случаи, когда ядерный и другой радиоактивный материал, находящийся вне регулирующего контроля, был фактически приобретен злоумышленниками.

3.12. Радиоактивные источники, находящиеся вне регулирующего контроля, могут быть просто обнаружены злоумышленниками или предложены для продажи злоумышленникам. Такие возможности следует учитывать при оценке вероятности приобретения злоумышленником материала, находящегося вне регулирующего контроля⁸. Злоумышленник может также, пусть и с меньшей долей вероятности, купить или иным образом приобрести готовое устройство, содержащее материал, находящийся вне регулирующего контроля, и эту возможность также следует учитывать при оценке угроз.

3.13. Следовательно, в оценку угрозы следует включать расчеты вероятности того, что нарушитель может приобрести материал, уже вышедший из-под регулирующего контроля, как внутри, так и за пределами государства, а также описания типов материала, которые могут быть приобретены. Расчет этой вероятности может потребовать от компетентного органа определения всех мест, где материал был изготовлен, использовался, хранился или транспортировался. Компетентный орган также должен знать общепринятые способы использования ядерного материала и другого радиоактивного материала в государстве, историю ведения государством учета и контроля

⁸ Также могут быть случаи, когда ядерный или другой радиоактивный материал, находящийся вне регулирующего контроля, перевозится без ведома перевозчика или грузоотправителя.

ядерного материала и реестров радиоактивных источников, а также иные механизмы контроля других радиоактивных материалов. Может быть оценена вероятность приобретения злоумышленником ядерных или других радиоактивных материалов, которые утеряны, пропали или были похищены. Поскольку данные о таких случаях по определению могут быть неполными или неточными, такую вероятность будет определить труднее, и поэтому, возможно, также потребуется рассчитать соответствующие границы неопределенности.

ТРАНСГРАНИЧНЫЕ ПЕРЕМЕЩЕНИЯ

3.14. В ITDB отражается информация о трансграничных перемещениях ядерного и другого радиоактивного материала, находящегося вне регулирующего контроля. Следовательно, вероятность приобретения злоумышленником ядерного или другого радиоактивного материала, находящегося вне регулирующего контроля, будет зависеть от доступности такого материала не только внутри государства, но и в любом другом месте.

3.15. Поэтому оценить угрозу, исходящую от материала, уже утратившего регулирующий контроль, сложно, поскольку у государства может не иметься детальной картины того, насколько вероятна доступность материала в других государствах. Для консервативной оценки количества доступного материала может использоваться информация из ITDB. Однако количество материала, находящегося вне регулирующего контроля, информация о котором не была передана в ITDB, неизвестно. При проведении оценки угрозы компетентный орган должен будет решить, какое значение придавать этому фактору.

3.16. В рамках оценки угроз на национальном уровне ответственному компетентному органу следует, помимо типов и количества материала, находящегося вне регулирующего контроля, учитывать возможные транзитные маршруты перемещения такого материала в государство и из него. Поэтому компетентному органу следует учитывать ядерный или другой радиоактивный материал, который:

- a) ввозится в государство или вывозится из него через установленные пункты пропуска (наземные, воздушные или водные), коммерческим транспортом или частными транспортными средствами;
- b) ввозится в государство или вывозится из него через неустановленные пункты пропуска;

- с) перемещается через территорию государства транзитом (т.е. ввозится в государство, но не предназначается для окончательной доставки внутри государства). Во многих случаях такой материал не идентифицируется и необязательно соответствует процедурам внутреннего контроля государства.

3.17. Компетентному органу следует учитывать возможность использования злоумышленником глобальной логистической цепи для незаконной перевозки ядерного и другого радиоактивного материала, находящегося вне регулирующего контроля. Внедрение эффективных систем и мер пограничного контроля в рамках архитектуры обнаружения событий, связанных с физической ядерной безопасностью, может способствовать пресечению, обнаружению или предотвращению трансграничных перемещений такого материала и значительно снизить уровень риска [11]. Эффективность государственных процедур и возможностей, равно как осведомленность о них злоумышленников будут влиять на уровень оцениваемой угрозы, связанной с материалами, приобретенными за пределами государства.

АНАЛИЗ ВОЗМОЖНОСТЕЙ И НАМЕРЕНИЙ ЗЛОУМЫШЛЕННИКА

3.18. В пунктах 3.10–3.17 говорится об оценке доступности ядерного и другого радиоактивного материала, находящегося вне регулирующего контроля, который может быть использован в преступных или преднамеренных несанкционированных действиях. Вероятность использования такого материала для совершения того или иного действия во многом зависит от потенциальных злоумышленников. В данном подразделе говорится об оценке злоумышленников путем оценки их возможностей (например, технических или финансовых) и их намерений (в частности, будут ли они использовать ядерный материал или другой радиоактивный материал, и если да, то как они могут его использовать и каким может быть их отношение к собственным радиологическим и другим рискам). Оценка злоумышленников — это динамичный процесс. Получить достоверную и актуальную информацию о возможностях и намерениях злоумышленника может быть сложно, а имеющаяся информация может быть противоречивой и неоднозначной. Эта сложность отчасти обусловлена мерами, предпринимаемыми злоумышленниками для сокрытия своей деятельности. Кроме того, злоумышленники адаптируются к меняющимся обстоятельствам, а изменения в оборонительной позиции государства

(например, усиление охраны конкретного объекта) обычно приводят к изменению вероятности совершения определенного действия конкретным злоумышленником. Эти изменения необязательно уменьшают или увеличивают общую вероятность; изменения могут лишь переключить внимание злоумышленника на другие цели или другие виды действий. Расчеты вероятности разных типов действий должны быть динамичными, при этом относительная вероятность будет меняться по мере усиления режима физической ядерной безопасности государства.

3.19. При проведении оценки злоумышленников первым шагом является идентификация потенциальных злоумышленников (как показано в столбце «Злоумышленники» на рис. 1). Компетентному органу, ответственному за оценку угроз и рисков, следует тесно взаимодействовать с правоохранительными органами и государственными разведывательными службами для выяснения того, какая информация имеется у государства о конкретном злоумышленнике. Информация также может передаваться государству в рамках двусторонних или многосторонних соглашений, а также поступать от международных правоохранительных организаций. Существует множество возможных мотивов для преступных или преднамеренных несанкционированных действий, равно как и множество потенциальных злоумышленников. Отождествление злоумышленников с отдельными лицами или конкретными группами позволяет более точно и конкретно охарактеризовать их намерения и возможности. В качестве альтернативы или в дополнение к вышесказанному распределение отдельных лиц или групп по категориям может обеспечить более эффективный анализ и позволит учесть в анализе некоторых ранее не известных злоумышленников.

3.20. Идентифицированных злоумышленников следует охарактеризовать на основе их вероятных намерений. Конкретные намерения часто находятся в сильной зависимости от общего мотива злоумышленника. Мотивы могут иметь финансовый, политический, идеологический или личный аспекты. Ключевые элементы этой характеристики:

- a) Готов ли злоумышленник применить ядерный или другой радиоактивный материал, находящийся вне регулирующего контроля, для совершения преступного или преднамеренного несанкционированного действия?
- b) Намерен ли злоумышленник совершить свое действие внутри государства?

- с) Намерен ли злоумышленник использовать государство в качестве плацдарма для совершения своего действия в другом государстве или против другого государства?

3.21. Вероятность того, что злоумышленник попытается совершить различные виды преступных или преднамеренных несанкционированных действий, может быть оценена количественно (в идеале как вероятностное распределение), но при необходимости оценки могут быть качественными (например, низкая, средняя или высокая вероятность). В любом случае при комплексной оценке угроз следует понимать и использовать фактор неопределенности в расчетах.

3.22. Помимо оценки возможных намерений злоумышленника совершить преступное или преднамеренное несанкционированное действие с использованием ядерного или другого радиоактивного материала, находящегося вне регулирующего контроля, следует оценить способность злоумышленника успешно совершить такое действие. При рассмотрении такой возможности часто выделяют две категории: организационные и логистические возможности. Злоумышленнику необходимо будет приобрести либо материал, регулирующий контроль над которым уже утрачен, либо материал, находящийся под регулирующим контролем, там, где он используется, хранится или перевозится. Оба варианта, вероятно, потребуют использования значительных ресурсов того или иного рода; например, доступ к материалам, находящимся вне регулирующего контроля, может быть относительно простым, если имеются достаточные финансовые средства, тогда как доступ к материалам, находящимся под регулирующим контролем, может потребовать большего объема технических или людских ресурсов. После того как материал будет приобретен, для создания устройства также потребуются соответствующая инфраструктура и специальные знания. Такие возможности часто строго контролируются и отслеживаются параллельно с обеспечением сохранности самих материалов, и злоумышленнику может быть сложно их получить. Компетентному органу следует оценить вероятность того, что такие возможности доступны внутри государства или могут быть получены за его пределами и затем перенесены в государство.

3.23. Задача оценки намерений и возможностей злоумышленников компетентным органом осложняется отсутствием исторических данных, которые можно было бы использовать для расчетов вероятности. Компетентный орган может произвести оценку намерений и возможностей злоумышленника на основе заявлений последнего, доказательств действий,

которые могли быть предприняты для нужд совершения преступного или преднамеренного несанкционированного действия, а также знания целей и предпочтений злоумышленника. Такая информация о злоумышленниках может считаться чувствительной, и ее следует защищать в соответствии с национальной политикой информационной безопасности. Хотя расчеты вероятности на основе таких данных могут быть весьма неопределенными, они все же могут дать относительно полное представление об угрозе со стороны разных злоумышленников или типов злоумышленников.

4. ИДЕНТИФИКАЦИЯ ЦЕЛЕЙ И ОЦЕНКА ПОТЕНЦИАЛЬНЫХ ПОСЛЕДСТВИЙ

4.1. Раздел 3 посвящен идентификации угроз, включая определение злоумышленников и средств совершения преступных или преднамеренных несанкционированных действий (использование ядерного или другого радиоактивного материала, находящегося вне регулирующего контроля, в устройствах). В данном разделе представлены руководящие указания по методам и подходам к идентификации и оценке целей и потенциальных последствий событий в области физической ядерной безопасности, связанных с ядерным и другим радиоактивным материалом, находящимся вне регулирующего контроля. Для выполнения комплексной оценки риска необходимо понимать привлекательность разных целей и вероятные последствия применения разных устройств против этих целей, поскольку вероятность того, что нарушитель попытается совершить действие против какой-либо цели, зависит от ценности выбранного подхода для данного конкретного злоумышленника.

4.2. В «Рекомендациях по физической ядерной безопасности, касающихся ядерных и других радиоактивных материалов, находящихся вне регулирующего контроля» [6], «цель» определяется как ядерные материалы, другие радиоактивные материалы, соответствующие установки, соответствующая деятельность или другие объекты или предметы, которые могут быть использованы при создании угрозы физической ядерной безопасности, включая крупные общественные мероприятия, стратегические объекты, чувствительную информацию и активы чувствительной информации. Поскольку настоящее практическое руководство посвящено ядерному и другому радиоактивному материалу, находящемуся вне регулирующего контроля, термин «цель» в контексте

настоящей публикации не охватывает материал, находящийся под регулирующим контролем, соответствующие установки и соответствующую деятельность.

ИДЕНТИФИКАЦИЯ ЦЕЛЕЙ

4.3. Цели могут быть идентифицированы очень конкретно (например, конкретное здание, памятник или событие) либо как класс (например, офисные здания, памятники, спортивные мероприятия или места в определенном городе). Для общей оценки угроз в отсутствие конкретной разведывательной информации идентификация конкретных целей приведет к составлению более длинного списка целей (которые затем следует расставить в порядке приоритетности), чем идентификация целевых классов. В случае, если конкретные цели внутри классов обладают свойствами, которые делают их намного более очевидными или вероятными, чем другие цели в том же классе, уместно применить сочетание конкретных целей и классов. Учитывая сложность приобретения ядерного материала или другого радиоактивного материала, а также относительную редкость устройств, содержащих такой материал, целесообразно ограничить список целей только теми, которые имеют наибольшую ценность (например, высокую вероятность успеха и большой эффект), и не включать в него все потенциальные цели.

4.4. При идентификации целей последствия для людей, имущества и окружающей среды могут учитываться в рамках следующих классов:

- a) здания, памятники или места, имеющие символическое значение: к таким объектам могут относиться правительственные здания, важные частные учреждения, памятники, дворцы, музеи, религиозные объекты или объекты, обладающие большой культурной ценностью или политической значимостью. Они также могут представлять ценность из-за своей принадлежности к другому государству (например, посольство или консульство);
- b) объекты критической инфраструктуры: такие объекты могут включать важнейшие предприятия энерго- и водоснабжения, места добычи природных ресурсов, транспортные узлы или коммуникации. Потенциально привлекательными целями могут быть плотины, электростанции, нефтеперерабатывающие заводы, водоочистные

сооружения, мосты или другие объекты, информационные системы и структуры, которые предоставляют необходимые услуги большому количеству людей;

- с) населенные пункты: густонаселенные районы могут быть привлекательными для злоумышленников, намеревающихся убить или покалечить людей или вызвать серьезный хаос. Целями могут также стать места компактного проживания определенных групп людей (например, этнических или религиозных групп);
- д) специальные мероприятия, которые имеют особое символическое значение и проходят с участием большого числа людей на небольшой территории, могут быть привлекательными для злоумышленников. К этому классу целей могут быть отнесены такие события, как крупные спортивные соревнования, политические митинги, национальные праздники или религиозные фестивали;
- е) экологические ресурсы или экосистемы.

4.5. Идентифицированные цели могут быть расставлены в порядке приоритетности исходя из предполагаемой вероятности их выбора, привлекательности для злоумышленника или потенциальных последствий нападения. Компетентному органу следует признать, что разные злоумышленники могут предпочитать разные цели — в зависимости от собственных устремлений и возможностей. Кроме того, одни цели могут быть более привлекательными, чем другие, с точки зрения типа события, связанного с физической ядерной безопасностью. Относительная привлекательность разных целей будет зависеть от устремлений злоумышленника и обычно бывает связана с желаемым эффектом, включая:

- а) затронутое население — кто и сколько;
- б) финансовые последствия нарушения нормальной жизнедеятельности и ущерба;
- с) экономическую или логистическую ценность цели;
- д) символическое значение цели.

4.6. Привлекательность также может зависеть от уязвимости цели (т.е. легкости, с которой она может быть атакована, легкости ухода и вероятности успеха). Таким образом, оценка привлекательности цели тесно связана с оценкой уязвимости цели и потенциальных последствий события, связанного с физической ядерной безопасностью. Относительная привлекательность целей может меняться со временем в зависимости от изменений в используемых средствах защиты или устремлениях злоумышленника.

ПОСЛЕДСТВИЯ СОБЫТИЙ, СВЯЗАННЫХ С ФИЗИЧЕСКОЙ ЯДЕРНОЙ БЕЗОПАСНОСТЬЮ

4.7. Последствия события, связанного с физической ядерной безопасностью, будут зависеть от характера, места и других обстоятельств события. Первоначальный прямой эффект от события может перерасти в последующие вторичные и третичные эффекты⁹. В случае совершения преступных или преднамеренных несанкционированных действий с ядерным и другим радиоактивным материалом следует оценить потенциальные последствия для людей (как правило, последствия для здоровья или общества), имущества (как правило, экономические последствия) и окружающей среды. При проведении оценки угроз следует осознать потенциальные последствия, а при выполнении оценки риска — оценить их с определенной степенью детальности. Пункты 4.7–4.18 посвящены оценке таких последствий.

4.8. В случае событий, связанных с физической ядерной безопасностью, потенциальные последствия для здоровья человека следует рассчитывать в рамках оценки риска. К ним могут относиться несчастные случаи (смерть и ранения), вызванные устройством (например, в результате взрыва), а также радиационным облучением или попаданием в организм радионуклидов от ядерного материала или другого радиоактивного материала, что может привести к смерти, серьезной травме или значительному ухудшению функции тканей или органа. Использование СЯУ может повлечь за собой радиационные эффекты от ядерного взрыва, а также нерадиологические эффекты от взрывной волны или теплового удара, а также долгосрочные радиологические эффекты, связанные с выпадением осадков.

4.9. Экономические издержки могут быть обусловлены многими аспектами события, связанного с физической ядерной безопасностью, но особенно необходимостью ликвидации последствий для людей, имущества и окружающей среды. Сюда могут входить расходы на лечение заболевших

⁹ Вторичные и третичные эффекты — это последствия, возникающие в результате события, связанного с физической ядерной безопасностью, но не являющиеся прямым следствием нападения. Например, подрыв РДУ в порту может иметь прямые последствия, такие как ранение людей и материальный ущерб, но может также привести к закрытию порта на время расследования и проведения восстановительных работ, что приведет к сокращению торговли и, возможно, к закрытию связанных с портом предприятий. Эти дополнительные последствия являются, соответственно, вторичным и третичным эффектом.

(или тех, кто опасается, что заболел), дезактивацию пострадавших территорий (или на вывоз и утилизацию почвы, строительных конструкций и содержимого зданий, которые невозможно легко дезактивировать), эвакуацию и переселение людей, а также на свертывание и восстановление работы предприятий. Помимо прямых издержек, событие может оказать косвенное воздействие на экономику государства.

4.10. В результате события, связанного с физической ядерной безопасностью, могут также иметь место экологические последствия. Радиоактивный материал может быть умышленно использован для загрязнения, например, почвы, подземных вод или уязвимых экологических зон, которые с трудом поддаются дезактивации, или же радионуклиды, рассеянные из устройства, могут попасть в окружающую среду. Вследствие загрязнения территории жители могут навсегда покинуть этот район, а сельскохозяйственная и другая промышленная продукция с этой территории перестанет пользоваться спросом. Длительный период полураспада некоторых радионуклидов означает, что воздействие загрязнения может сохраняться в течение длительного времени.

4.11. Наконец, преступные или преднамеренные несанкционированные действия могут иметь социальные последствия для государства, региона или всего мира. Могут иметь место вспышки недовольства или проявления паники среди затронутых лиц или сообществ. На местном уровне может иметь место эвакуация отдельных районов, а позже — их оставление населением. На национальном уровне событие может прервать политический процесс (например, выборы) или повлиять на него. Социальные последствия могут также выйти за пределы государства, в котором произошло событие, например в результате нарушения логистических цепочек, массового перемещения людей или дипломатических осложнений. Эти последствия чрезвычайно трудно предсказать или количественно оценить, и во многих

случаях масштаб последствий зависит в равной степени как от самого акта, так и от реакции на него со стороны властей. Поэтому при попытках оценить такие последствия следует проявлять большую осторожность¹⁰.

4.12. Последствия могут быть оценены несколькими способами, включая качественное ранжирование и детальное моделирование последствий.

4.13. Качественное ранжирование последствий предполагает, что соответствующие эксперты распределяют потенциальные последствия по категориям на основе их качественной характеристики, такой как «тяжелые», «умеренные» и «минимальные». Пример матрицы последствий с четырьмя разными типами эффектов и пятью категориями ранжирования приведен в таблице 1.

4.14. Метод качественного ранжирования обычно предполагает использование общих категорий, описывающих последствия события, связанного с физической ядерной безопасностью, для людей, имущества и окружающей среды. Масштаб последствий, описываемых этими категориями, может различаться на порядки (например, как в строке «влияние на здоровье» в таблице 1). Целью должно быть выделение достаточно широких категорий для того, чтобы соответствующие эксперты могли выбрать правильную категорию для описания последствий события, и сохранение при этом значимых различий между разными категориями. Так, достаточно широкие категории могут допускать неопределенность при оценке последствий, обеспечивая при этом, чтобы события уверенно вносились в правильную категорию. В определениях категорий могут быть включены количественные критерии некоторых типов последствий, таких как последствия для здоровья, экономики и окружающей среды, в то время как другие категории, такие как социальные последствия, вероятно, будут определяться только качественными показателями. Такой подход позволяет оценивать неодинаковые элементы последствий в рамках единой системы. Однако при выделении категорий следует проявлять осторожность, чтобы

¹⁰ Также стоит отметить, что четыре описанные категории последствий — медицинские, экономические, экологические и социальные — не являются взаимоисключающими. Последствия одной категории могут оказывать прямое воздействие на последствия другой категории. Например, беспокойство людей, живущих рядом с местом взрыва (социальные последствия), вызванная радиоактивным загрязнением в результате взрыва (экологические последствия), может привести к оставлению людьми данного района и свертыванию коммерческой деятельности (экономическое воздействие).

ТАБЛИЦА 1. ПРИМЕР МАТРИЦЫ ПОСЛЕДСТВИЙ С КАЧЕСТВЕННЫМ РАНЖИРОВАНИЕМ

Элементы последствий	1	2	3	4	5
Эффект для здоровья	Вероятно, не приведет к человеческим жертвам	Вероятно, приведет к жертвам в количестве менее 10	Вероятно, приведет к жертвам в количестве более 10	Вероятно, приведет к жертвам в количестве более 100	Вероятно, приведет к жертвам в количестве более 1000
Экономический эффект	Издержки, равные стоимости замены здания	Значительные издержки в масштабе городского района	Значительные издержки в масштабе города	Издержки в размере от 1% до 10% ВВП ^а	Издержки в размере более 10% ВВП ^а
Экологический эффект	Без значительного загрязнения	Небольшое по площади или временное загрязнение	Значительное загрязнение на небольшой площади	Большая площадь с ощутимым загрязнением или небольшая площадь с недоступными критически важными ресурсами	Большая площадь с недоступными критически важными ресурсами вследствие загрязнения
Общественный эффект	Без серьезных изменений в поведении населения или влияния на жизнь общества на местном или национальном уровне	Эпизодическая или незначительная потеря неосновных социальных функций в пределах ограниченной географической зоны	Потеря многих неосновных социальных функций в пределах ограниченной географической зоны	Нарушение и обой важных социальных функций в течение длительного периода	Утрата доверия к правительству и государственным институтам Повсеместное игнорирование официальных предписаний Повсеместное мародерство и гражданские беспорядки

Примечание: Цифры и описания носят лишь приближительный характер и должны корректироваться с учетом национальных условий и приоритетов.

^а ВВП: валовой внутренний продукт.

последствия, описываемые одними и теми же качественными критериями, имели сопоставимый масштаб для каждого типа последствий. Такой подход известен как градуировка шкалы для разных типов. Также важно обеспечить, чтобы категории на шкале ранжирования отражали все уровни последствий: распространенной ошибкой является помещение самой высокой категории на слишком низкий уровень, в результате чего экстремальные последствия будут неотличимы от серьезных последствий.

4.15. Детальное моделирование последствий представляет собой попытку смоделировать эффекты от действий, выбранных злоумышленником (например, применение устройства), на объекте, являющемся целью. Оценки таких факторов, как воздействие взрыва, рассеивание радиоактивных материалов, распределение индивидуальных и коллективных доз среди населения, а также, среди прочего, уровни и масштабы загрязнения, выполняются при помощи математических моделей событий, а не субъективных оценок. Эти модели могут быть очень простыми (например, радиус взрыва и равномерное рассеивание по затронутому квадранту с учетом направления ветра) или очень детальными (например, модель воздушных потоков на основе расчета гидродинамических характеристик) и должны, где это возможно, основываться на эмпирических данных. На практике, даже когда используются детальные модели, в расчетах уровня последствий обычно присутствует значительная неопределенность, связанная с непредсказуемостью таких факторов, как скорость и направление ветра, и поэтому расчеты обычно имеют относительно широкий диапазон погрешностей.

4.16. Конечными результатами оценки последствий являются, как правило, число жертв и экономические издержки события, связанного с физической ядерной безопасностью. Иногда число жертв и экономические издержки события, связанного с физической ядерной безопасностью, объединяются посредством расчета номинальной денежной стоимости каждой жертвы (например, стоимости статистической жизни¹¹) и прибавления результата к экономическим издержкам.

4.17. Оценка социальных последствий представляет собой трудную задачу. Хотя при любой оценке угроз безусловно важно учитывать воздействие на общество — причем на практике социальные последствия могут быть

¹¹ Понятие стоимости статистической жизни выражает сумму, которую люди готовы заплатить за снижение риска до такой степени, чтобы от источника риска погибло в среднем на одного человека меньше.

основной целью для злоумышленника и иметь наибольшее значение для государства, — социальные последствия чрезвычайно трудно оценить, даже качественно. Кроме того, на социальные последствия может существенно повлиять реакция государства на событие, связанное с физической ядерной безопасностью, и они, таким образом, не полностью определяются самим событием. Общепринятого метода оценки социальных последствий не существует. Поэтому государствам необходимо будет выработать свои собственные подходы к учету социальных эффектов при оценках последствий.

4.18. Поскольку последствия зависят от использованного радиоактивного материала, характеристик устройства, характеристик цели, эффективности реагирования, а также присутствия людей и имущества и характера окружающей среды вблизи цели, расчет последствий может охватывать широкий диапазон. Поэтому для различения разных сценариев вполне достаточно использовать оценки последствий, отличающиеся на один порядок. При простом анализе последствия могут оцениваться в виде уровней (например, от 1 до 5 или в виде качественных описаний категорий, как указано в таблице 1), а для численных расчетов может использоваться цифра, представляющая собой основную оценку экономического воздействия. В иных случаях из расчетов последствий могут быть исключены все единицы измерения, и для обозначения относительных последствий может использоваться «стандартизированный рейтинг воздействия». Стандартизированный рейтинг воздействия используется для демонстрации относительных уровней воздействия без указания конкретных денежных сумм.

5. МЕТОДИКИ ОЦЕНКИ УГРОЗ И РИСКОВ

5.1. В разделах 3 и 4 были описаны составляющие оценки угроз и рисков. В данном разделе описываются общие методы объединения этих составляющих в оценки, которые имели бы практическое значение. На рис. 2 показаны составляющие угрозы и риска и взаимосвязь между ними. При таком использовании угроза обычно включает в себя намерения и возможности и определяется потенциальными последствиями и вероятностью успеха (с точки зрения злоумышленника) конкретного типа события, связанного с физической ядерной безопасностью. Риск является производной от угрозы, уязвимости и последствий и может быть выражен

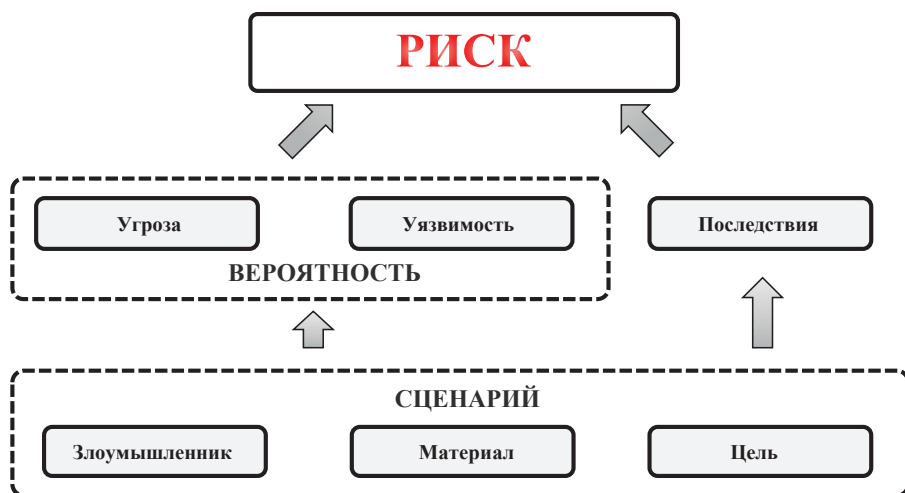


РИС. 2. Взаимосвязь между угрозой и риском и дополнительными элементами.

количественно — например, как ожидаемый ущерб (последствия в год), или качественно — с использованием относительных показателей (например, низкий, средний и высокий). Поскольку расчет риска зависит от расчета угрозы, уязвимости и последствий, оценка угроз обычно выполняется до оценки риска и служит основой для нее.

5.2. Существует множество типов оценок угроз и рисков, а также множество методик, подходящих для различных ситуаций. Конкретно выбранную методику следует адаптировать к конкретным оцениваемым ситуациям, а также к имеющимся ресурсам и техническим возможностям. Важно определиться с тем, какие показатели оценки будут применяться — качественные или количественные. Как правило, если для принятия решений об установлении приоритетов достаточно качественной оценки (например, низкая, средняя и высокая), то следует использовать качественные методы. Однако при необходимости более точной характеристики угроз или рисков или более четкого разграничения угроз и рисков следует отдать предпочтение количественным методикам.

5.3. Существуют также разные уровни оценки угроз и рисков, наиболее распространенными из которых являются стратегический и тактический. Стратегические оценки охватывают более длительные временные интервалы и сосредоточены на управлении ресурсами и разработке планов по улучшению возможностей. Тактические оценки обычно

выполняются в условиях серьезного дефицита времени и используются для обоснования оперативных решений в конкретных случаях. Поскольку настоящая публикация посвящена оценкам угроз и рисков, применяемых для обоснования разработки и внедрения мер физической ядерной безопасности, описанные здесь оценки носят стратегический характер.

5.4. Оценка угроз физической ядерной безопасности отличается от оценок других угроз по ряду причин. Например, научно-технические характеристики ядерного материала и другого радиоактивного материала оказывают существенное влияние на характер и уровень угрозы по сравнению с обычными видами оружия — огнестрельным оружием и взрывчатыми веществами. Кроме того, определяющим аспектом оценки угрозы является доступность и потенциальное использование ядерного материала и другого радиоактивного материала, что предполагает более узкий и конкретный охват по сравнению, скажем, с преступным или преднамеренным несанкционированным действием, связанным с приобретением огнестрельного оружия. Более того, небольшое число событий, связанных с физической ядерной безопасностью, означает, что эмпирическая база для точной оценки как угрозы, так и риска ограничена.

МЕТОДИКИ ОЦЕНКИ УГРОЗ

5.5. Для выполнения оценки угроз используется ряд методов. Два общепринятых метода состоят в следующем:

- а) подход, основанный на описании угроз: качественный метод описания уровня и характеристик угроз;
- б) подход, основанный на ранжировании угроз: полуколичественный метод расчета составляющих угроз и объединения их в общую оценку угрозы.

Эти методики могут применяться по отдельности или в сочетании друг с другом. Описательный подход дает описание угрозы, которое можно эффективно использовать для оценки уровня угрозы и применения методики качественной оценки риска. Поскольку он не предполагает количественных расчетов, его нельзя использовать с методом количественной оценки риска, если он не будет дополнен методом проведения количественных расчетов. Подход, основанный на ранжировании угроз, может использоваться

как с качественными, так и с количественными методиками оценки риска, поскольку ранжирование можно легко преобразовать в оценки относительной вероятности.

5.6. В обоих случаях методика основывается на общем трехступенчатом цикле, аналогичном тому, который представлен на рис. 3. На первой ступени цикла компетентный орган планирует проведение оценки угроз, собирает новые или существующие источники информации об угрозах, оценивает качество и достоверность информации и сопоставляет информацию, относящуюся к одним и тем же угрозам, событиям или действиям. Вторая ступень — это проведение анализа, в ходе которого информация интегрируется и интерпретируется для формирования связного массива знаний. На последней стадии оценки угроз компетентный орган, ответственный за оценку угроз, оценивает относительный уровень или вероятность угроз, рассматриваемых в оценке, и составляет описание угроз или проводит их ранжирование.

Подход, основанный на описании угроз

5.7. Подход, основанный на описании угроз, дает качественную оценку угрозы. Соответствующие эксперты готовят подробную сводку информации о намерениях, возможностях и мотивах злоумышленников. Оценка угроз дает представление об организации, возможностях, операциях и

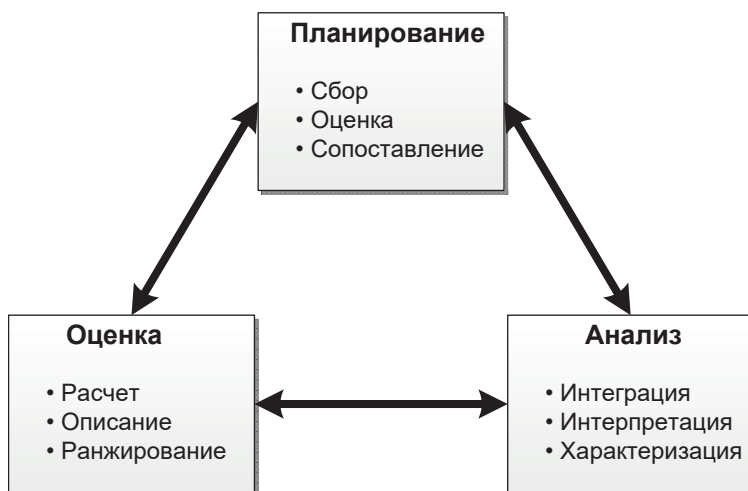


РИС. 3. Процесс оценки угрозы с указанием ключевых видов деятельности.

механизмах поддержки злоумышленников. Такая информация полезна при оценке вероятных типов действий, целей и средств выполнения действий различными злоумышленниками.

5.8. В описательном подходе используется набор стандартных методов, направленных на разработку гипотез, реконструкцию хода отдельных событий, связанных с физической ядерной безопасностью, выявление серии связанных событий, понимание того, как организованы злоумышленники, и анализ масштабов и закономерностей связанных с ними действий. Это позволяет аналитику включать дополнительные оценки и замечания для учета неопределенности и непредсказуемости, а также дополнять неполную информацию [15].

5.9. Описательный подход включает два основных метода: анализ событий, связанных с физической ядерной безопасностью, и анализ конкретных характеристик злоумышленника. Анализ событий, связанных с физической ядерной безопасностью, имеет целью выявление тенденций и признаков, указывающих на предпочтения, на базе информации об известных событиях. События могут рассматриваться с точки зрения типа использованного радиоактивного материала, места происшествия, уровня возможностей и характера действий злоумышленника. Анализ конкретных характеристик злоумышленника включает рассмотрение намерений, возможностей, организационных структур и финансовых ресурсов злоумышленников, а также их прошлой деятельности, предпочтений и наклонностей.

5.10. Методы, обеспечивающие такой анализ, включают использование географических информационных систем для выявления взаимосвязей между местонахождением злоумышленников, событиями, связанными с физической ядерной безопасностью, и соответствующими действиями, интегрированных баз данных для понимания таких взаимосвязей и диаграмм связей между отдельными лицами и группами (например, инструментов для анализа социальных сетей). Примеры некоторых из этих методов можно найти в приложении II.

5.11. Результатом применения описательного подхода является описание конкретных характеристик и наклонностей злоумышленника. Пример анализа совокупности условных злоумышленников приведен в таблице 2.

Подход, основанный на ранжировании угроз

5.12. Подход, основанный на ранжировании угроз, дает возможность оценить угрозу количественно. Этот метод сочетает расчет относительной вероятности угроз с текстовыми описаниями типов угроз, используя комбинацию расчетных шкал с качественными дескрипторами, также известными как «метаграммы». В нем используется тот же подход к получению общего представления об угрозе, что и в описательном подходе, но на оценочном этапе ранжирования угроз производится расчет относительной вероятности разных аспектов угрозы. Эти аспекты обычно включают в себя возможности и намерения и могут также включать в себя другие аспекты события, связанного физической ядерной безопасностью, такие как типы материалов, типы устройств или типы целей. Результаты оценки этих составляющих угрозы затем объединяются в общий «рейтинг угрозы» по заранее определенной методике. Методика, используемая для объединения оценок разных составляющих угрозы, должна быть математически обоснованной. Важно отметить, что при количественной оценке угроз в сфере физической ядерной безопасности шкалы оценки различных угроз (или составляющих угрозы), вероятнее всего, будут градуироваться относительно друг друга, но не относительно какого-либо другого типа угроз. Таким образом, угроза физической ядерной безопасности, оцененная как «высокая», может быть низкой по сравнению с угрозой других типов нападений, например с использованием взрывчатых веществ и огнестрельного оружия. С другой стороны, при комплексной оценке опасностей угрозы, связанные с физической ядерной безопасностью, оцениваются наряду с другими угрозами.

ТАБЛИЦА 2. ПРИМЕР РЕЗУЛЬТАТОВ ОЦЕНКИ УГРОЗ
В ОПИСАТЕЛЬНОЙ ФОРМЕ

Угрозы	Намерения	Возможности
Группа А	Если бы группа А располагала материалом, то, вероятнее всего, использовала бы его для создания РДУ с целью загрязнения городской территории и причинения высокого экономического ущерба. При этом маловероятно, что она займется какой-либо деятельностью, которая приведет к большому числу жертв.	Группа А имеет контакты с наркоторговцами и организованной преступностью и, благодаря этим контактам либо самостоятельно, имеет возможность приобретать радиоактивный материал.

ТАБЛИЦА 2. ПРИМЕР РЕЗУЛЬТАТОВ ОЦЕНКИ УГРОЗ
В ОПИСАТЕЛЬНОЙ ФОРМЕ (продолжение)

Угрозы	Намерения	Возможности
Группа В	Группа В не стремится к массовым жертвам, но, как известно, проводит избирательные нападения. Избирательное загрязнение продуктов питания или источников водоснабжения соответствовало бы типичной тактике группы В.	Группа В имеет контакты с группировками, занимающимися контрабандой, и организованной преступностью и, благодаря этим контактам либо самостоятельно, имеет возможность приобретать радиоактивный материал.
Группа С	Группа С заинтересована практически в любом нападении, которое вызовет серьезный хаос, разрушения или массовые жертвы. Она уже предпринимала подобные нападения в прошлом и ответственна за ряд спланированных нападений, которые были предотвращены. Группа С заинтересована в приобретении радиоактивного материала для создания РДУ. Если бы они могли приобрести материал и сконструировать СЯУ или приобрести уже готовое ядерное устройство, то взорвали бы его в городском населенном пункте.	Ограниченные контакты с организованной преступностью и контрабандистами снижают возможности группы С для приобретения материалов или устройств через незаконных поставщиков. Группа располагает достаточными ресурсами, чтобы представлять значительную угрозу прямого хищения материалов с установки или в ходе деятельности, находящейся под регулирующим контролем.

Примечание: Все описания носят гипотетический характер. СЯУ — самодельное ядерное устройство; РДУ — радиологическое диспергирующее устройство.

5.13. Важнейшим элементом подхода, основанного на ранжировании угроз, является процесс ранжирования. При выполнении этого процесса принято запрашивать данные от соответствующих экспертов и вкладывать четко определенный смысл в разные оценки. Ранжируемые атрибуты (критерии, факторы или категории) должны быть ортогональными, то есть они не должны пересекаться таким образом, чтобы определенные составляющие угрозы учитывались дважды. Для каждого ранжируемого атрибута обычно применяются отдельные оценочные шкалы. Например, могут применяться отдельные шкалы для «финансовых ресурсов» и «технических

возможностей», которые затем следует учитывать независимо. Для объяснения каждого уровня шкалы принято использовать текстовые описания. Чаще всего используются шкалы с пятью, семью или десятью уровнями, которые обеспечивают дифференциацию, не усложняя процесс оценки, но количество уровней само по себе не является показателем правильности или точности, поскольку неопределенность в оценках сохранится. Документирование неопределенности или достоверности каждого рейтинга остается важным аспектом оценки.

5.14. Рейтинги злоумышленников по каждому атрибуту объединяются в общий рейтинг каждого нарушителя и дают картину угрозы в целом. Существует множество различных подходов, которые можно использовать для объединения рейтингов, в зависимости от конкретной методики ранжирования. Ниже описаны наиболее распространенные из них.

- a) Высший рейтинг: Для определения общего рейтинга угрозы от злоумышленника применяется высший рейтинг по каждому атрибуту. Этот подход дает консервативную оценку угроз и основывается на уверенности в том, что злоумышленники будут стремиться уменьшить свои слабости, и поэтому можно ожидать, что их рейтинги атрибутов в областях с более низкими оценками повысятся.
- b) Средний рейтинг: Оценки различных атрибутов усредняются, часто путем использования числовых значений (например, по шкале от 1 до 5) в отдельных расчетах и выбора среднего значения. Этот подход придает равный вес каждому атрибуту. Значение, наиболее близкое к среднему, используется в общем рейтинге угрозы. Этот подход склонен занижать влияние очень высоких или очень низких рейтингов по определенным атрибутам, которые на самом деле могут заслуживать более тщательного изучения.
- c) Низший рейтинг: Для определения общего рейтинга угрозы от злоумышленника применяется низший рейтинг по каждому атрибуту. Этот подход предполагает, что низший рейтинг представляет собой наиболее серьезное препятствие, которое придется преодолеть злоумышленнику, и основывается на уверенности в том, что злоумышленник не сможет добиться успеха, не преодолев это препятствие.
- d) Преобразование в вероятность: Оценки преобразуются в значения вероятности для каждого атрибута (например, мотива, возможностей и намерений), часто с границами неопределенности, которые перемножаются для получения общей вероятности для данного злоумышленника. При использовании такого подхода необходимо

проявлять особую осторожность, следя за тем, чтобы значения вероятности определялись достаточно хорошо, чтобы обеспечить значимые различия между угрозами. Например, некоторые оценки могут потребовать проведения различия между редкими событиями (например, событиями, связанными с физической ядерной безопасностью) и более частыми событиями (например, наводнениями или землетрясениями). В этом случае вероятности могут различаться на несколько порядков.

- е) Взвешивание отдельных показателей: В этом подходе рейтинги угроз объединяются, как и в методе среднего рейтинга, но рейтингам по разным атрибутам присваивается разный вес — в зависимости от их предполагаемого значения для общей угрозы. (Напомним, что при усреднении всем атрибутам присваивается одинаковый вес.) Например, можно допустить, что для успешного совершения нападения злоумышленнику важнее иметь достаточные технические возможности, чем прочную организационную базу. В этом случае оценка технических возможностей должна иметь большее влияние на общий рейтинг угрозы, и поэтому рейтингу технических возможностей следует присвоить больший вес при расчете «среднего» показателя.

5.15. Важным преимуществом составления рейтингов угроз является то, что их можно преобразовать или интерпретировать как оценки вероятности, а такие оценки могут лечь в основу методик количественной оценки риска. Пример составленной шкалы угроз приведен в таблице 3. Представленные описания также могут применяться при подходе, основанном на описании угроз. Пример процесса ранжирования угроз и метаграммы представлен в приложении II.

ТАБЛИЦА 3. ПРИМЕР МЕТАГРАММЫ, ОПИСЫВАЮЩЕЙ ОБЩИЕ УРОВНИ УГРОЗ

Рейтинг оценки угрозы	Описание
Очень высокий	У злоумышленников имеются ранее созданные возможности и намерение немедленно атаковать цель Нападение оценивается как весьма вероятное

ТАБЛИЦА 3. ПРИМЕР МЕТАГРАММЫ, ОПИСЫВАЮЩЕЙ ОБЩИЕ УРОВНИ УГРОЗ (продолжение)

Рейтинг оценки угрозы	Описание
Высокий	<p>У злоумышленников имеется возможность атаковать цель, и такое нападение входит в текущие намерения группы</p> <p>Нападение оценивается как вероятное</p>
Средний	<p>У злоумышленников имеются некоторые возможности для того, чтобы атаковать цель, и такое нападение будет соответствовать намерениям группы, либо же у них есть такая возможность, но их намерение может зависеть от текущих обстоятельств</p> <p>Нападение оценивается как возможное</p>
Низкий	<p>В настоящее время у злоумышленников имеется мало возможностей и/или недостаточно сильное намерение атаковать цель</p> <p>Нападение оценивается как маловероятное</p>
Очень низкий	<p>В настоящее время у злоумышленников не имеется возможностей и/или намерения атаковать цель</p> <p>Нападение оценивается как крайне маловероятное</p>

МЕТОДИКИ ОЦЕНКИ РИСКОВ

5.16. В области физической ядерной безопасности риск обычно рассматривается как производная от трех компонентов: угрозы, уязвимости и последствий. Оценка риска представляет собой сочетание оценки вероятности наступления конкретных событий, связанных с физической ядерной безопасностью, выраженной в виде угрозы и уязвимости, с оценкой последствий таких событий, на основе чего выводится общий показатель, который полезно использовать при проектировании или совершенствовании систем и мер физической ядерной безопасности. Конкретное событие, связанное с физической ядерной безопасностью, может считаться «высокорисковым», если его наступление вероятно, если оно приведет к значительным последствиям или при соблюдении обоих условий. Оценивая ожидаемые значения экономических убытков из-за возможных событий, связанных с физической ядерной безопасностью, оценка рисков может дать

результаты, которые в некоторых случаях могут сравниваться со стоимостью систем и мер для предотвращения событий, связанных с физической ядерной безопасностью, с целью оценки экономической эффективности этих систем и мер. На практике такие сравнения необходимо проводить с большой осторожностью, чтобы должным образом учитывать неопределенность в оценке рисков и не создавать впечатление, что эти оценки более надежны или точны, чем они есть на самом деле, тем самым вводя в заблуждение компетентные органы, ответственные за осуществление таких мер.

5.17. Как и в случае с оценкой угроз, уровень детальности и сложности, а также объем количественного анализа при оценке рисков должен быть соразмерен с важностью решений об установлении приоритетов, которые она призвана подкреплять. Различным областям исследований присущи различные методики оценки рисков. В этом подразделе описываются два метода, которые обычно используются и считаются подходящими для определения приоритетности при внедрении систем и мер физической ядерной безопасности — один качественный и один количественный. Это следующие методы:

- a) составление реестра рисков: отображение идентифицированных сценариев в виде матрицы со шкалами вероятности и последствий для сравнительной визуализации рисков. Эта методика может быть качественной или полуквантитативной;
- b) вероятностная оценка риска: сценарный подход, в котором формируются сценарии путем объединения основных элементов или «шагов», ведущих к событию с последствиями (обычно отображаемых графически в виде дерева событий, дерева решений или дерева ошибок) и оценки конечных последствий для каждого из определенных сценариев. Этот подход объединяет количественные расчеты вероятности (или правдоподобности) для каждого основного элемента (называемого «узлом» дерева событий) для получения общих значений вероятности сценариев. Эта методика аналогична вероятностной оценке ядерной безопасности [16].

5.18. Оба указанных подхода, но особенно последний, опираются на использование математических моделей для отображения возможных событий и на заключения соответствующих экспертов при определении вероятностей (в тех случаях, когда они не могут быть получены из эмпирических наблюдений за частотой), а также других параметров [17].

Ниже описываются ключевые принципы оценки риска с привлечением соответствующих экспертов или использованием моделей и учетом неопределенности в оценках и результатах.

5.19. Международные отраслевые стандарты менеджмента рисков определяют три ключевых этапа оценки рисков: идентификация риска, анализ риска и оценка риска [7]. Хотя в методиках оценки рисков, представленных в данной публикации, эти наименования прямо не используются при описании каждого этапа, все три этапа в них присутствуют. Идентификация рисков осуществляется путем выбора сценария или разработки сценария в ходе обсуждения методики. Анализ рисков в целом проводится посредством оценки вероятностей и выполнения расчетов риска. Оценка рисков выполняется посредством описания анализа неопределенности и анализа чувствительности.

Методика составления реестра рисков

5.20. Реестр рисков — это перечень или каталог идентифицированных рисков, аналогичный реестру рисков в управлении проектами. В нем фиксируется риск, тяжесть последствий и вероятность их наступления, а также действия, которые необходимо предпринять для снижения риска. Для каждого общего риска обычно выполняется анализ наихудшего сценария, результатом чего является составление небольшого числа правдоподобных репрезентативных сценариев. Однако при некоторых методах применяется стандартный набор общих (или номинальных) сценариев с наибольшей вероятностью реализации. Такие сценарии могут служить эталоном для сравнительных оценок внутри одного типа и между разными типами сценариев риска. Тяжесть последствий, отраженных в рисках, часто имеет несколько аспектов и может частично или полностью охватывать следующие аспекты: человеческие жертвы, экономические убытки, социальные потрясения и ущерб окружающей среде.

5.21. Реестры рисков часто используются для сравнения разнородных, общих типов риска (например, стихийных бедствий, событий, связанных с физической ядерной безопасностью, и промышленных аварий) и помогают в распределении бюджетных средств между мероприятиями по ликвидации всех опасностей. Реестры рисков часто ведутся на высоком уровне (то есть на стратегическом уровне), где оценки относительной вероятности и тяжести даются соответствующими экспертами с использованием логарифмических шкал.

5.22. В реестр рисков следует включать указанные ниже компоненты.

- a) Сроки: поскольку реестр является документом, который регулярно обновляется, важно фиксировать момент, когда оценивались риски, и период, в течение которого такие оценки действительны. В случае изменения угрозы или изменения мер, принятых для снижения рисков, может произойти изменение риска. Эти изменения следует по мере необходимости включать в будущие оценки.
- b) Описание риска: поскольку в реестрах рисков используется небольшое число репрезентативных сценариев, в описание риска следует включать все параметры, которые определяют каждый идентифицированный сценарий и которые использовались для оценки риска. Среди них:
- предположения относительно цели;
 - тип устройства;
 - количество использованного материала;
 - возможности злоумышленника;
 - любые предположения, опирающиеся на заключения о вероятном качестве исполнения устройства (например, его надежности, эффективности или мощности);
 - предполагаемая последовательность событий, ведущих к событию, связанному с физической ядерной безопасностью;
 - соответствующие условия во время события (например, погодные условия или затрагиваемое население);
 - вероятная эффективность мер по смягчению последствий.
- c) Вероятность или частота возникновения: это оценка того, насколько вероятно, что событие произойдет (выражается в виде вероятностей или шансов, например низкая (<30%), средняя (31–70%) или высокая (>70%) вероятность), или как часто оно может происходить (выражается как частота, например 10 раз в год, один раз в год, один раз в 10 лет, один раз в 100 лет). Вероятность событий может быть оценена по абсолютной шкале, если это необходимо, но обычно важнее (и часто надежнее) оценивать события с точки зрения относительной частоты или вероятности (например, ядерный терроризм гораздо менее вероятен, чем наводнение, и гораздо более вероятен, чем уничтожение Земли астероидом). В зависимости от задачи, для оценки рисков может быть достаточно относительной шкалы.
- d) Тяжесть последствий: это оценка возможных последствий события, связанного с физической ядерной безопасностью. Может включать несколько отдельных оценок разных последствий, и они могут быть сведены в единую общую оценку. Как и в случае с вероятностью,

относительные показатели тяжести последствий могут быть более важными (и удобными для использования), чем абсолютные оценки последствий.

- е) Дополнительные меры противодействия: это действия, которые следует предпринять для предотвращения или уменьшения последствий события. Они могут включать плановые действия по реагированию, которые уже приняты во внимание при расчетах вероятности и тяжести последствий. Они также могут содержать возможные конкретные действия, которые могут быть предприняты для снижения либо вероятности, либо тяжести последствий конкретных событий. В последнем случае использование мер противодействия часто отображается в виде стрелки на диаграмме реестра рисков, показывающей размер и направление снижения риска, которое может обеспечить такая мера.

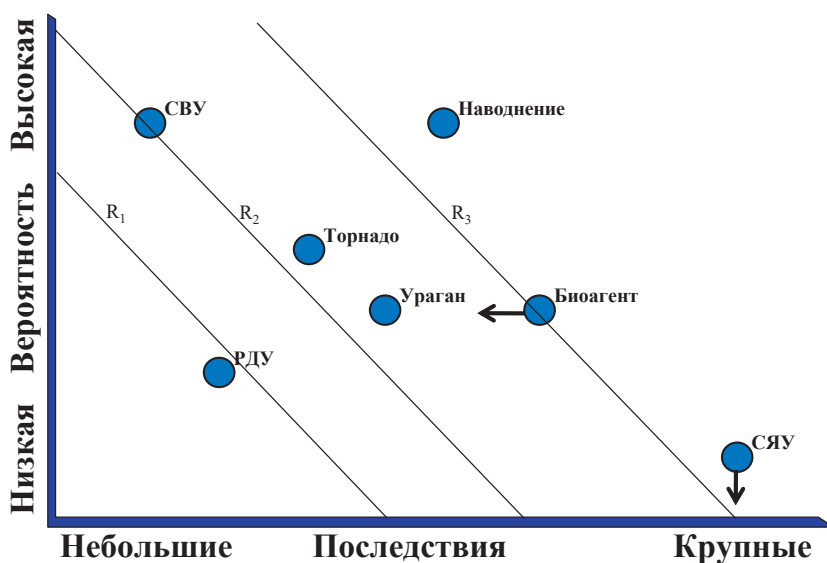
5.23. На рис. 4 показан пример диаграммы реестра рисков с условными данными. В этом примере диаграмма показывает, что сценарий с использованием СЯУ имеет наибольшие последствия, но наименьшую вероятность. Наводнения могут иметь примерно такую же степень вероятности, как и использование самодельных взрывных устройств (СВУ), но с гораздо большими последствиями. Стрелка на символе нападения с применением биологического агента («биоагента») указывает на потенциальное снижение последствий (но не вероятности) за счет использования конкретной медицинской меры противодействия. Стрелка, отходящая от символа СЯУ, указывает на снижение вероятности (но не последствий) нападения с использованием СЯУ, которое может быть достигнуто за счет введения улучшенных мер физической ядерной безопасности. Другие меры или их комбинации могут уменьшить как вероятность, так и последствия. В таких случаях стрелки будут указывать по диагонали на новую вероятность и последствия, связанные с уменьшенным риском. Наконец, диагональные линии — это линии равного риска: все точки на линии имеют одинаковый рейтинг риска. Такие линии могут помочь руководителям при сравнении разных сценариев с одинаковым уровнем риска.

Методика вероятностной оценки риска

5.24. Вероятностная оценка риска может использоваться для количественной или полуколичественной оценки риска при различных заданных сценариях. При оценке рисков событий, связанных с физической

ядерной безопасностью, сценарии обычно строятся из ключевых элементов, представляемых, как правило, в виде дерева отказов, дерева событий или дерева решений.

5.25. Подход, основанный на вероятностной оценке риска, обеспечивает системный метод построения сценариев риска за счет определения важных элементов события, связанного с физической ядерной безопасностью, и создания «сценарного пространства», охватывающего все возможные случаи для каждого из элементов. Важными элементами могут быть такие обстоятельства, как решения злоумышленника о выборе конкретного порядка действий из числа возможных вариантов, успех или неудача промежуточных шагов в цепочке действий злоумышленника или эффективность (либо неэффективность) мер физической ядерной безопасности в предотвращении действий злоумышленника. Эти элементы

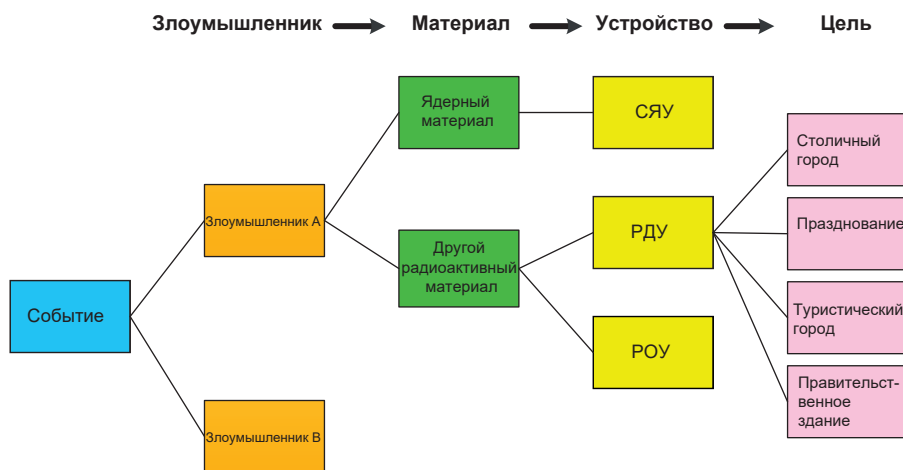


Примечание: Все расчетные значения вероятности и последствий являются условными и не отражают реальных значений. $R_1 < R_2 < R_3$ (линии обозначают одинаковый риск). СВУ — самодельное взрывное устройство; СЯУ — самодельное ядерное устройство; РДУ — радиологическое диспергирующее устройство.

РИС. 4. Пример реестра рисков с учетом всех опасностей, используемого для распределения ресурсов между мероприятиями по ликвидации всех опасностей.

могут быть описаны и представлены как точки ветвления на дереве событий, где разные пути движения по дереву отображают отдельные несхожие сценарии. Каждая точка ветвления называется узлом или уровнем дерева. Конечные узлы дерева (от которых не происходит дополнительного ветвления), иногда называемые листьями, отображают разные конечные результаты. При расчете риска последствия для каждого из конечных узлов дерева оцениваются по отдельности. Компетентному органу следует определить, какие последствия он считает релевантными и требующими оценки (например, человеческие жертвы, загрязнение окружающей среды, экономические последствия и социальные последствия). Вероятность любого сценария рассчитывается как производная от вероятностей для каждой из ветвей дерева, составляющих этот сценарий.

5.26. Дерево строится путем определения различных возможностей для каждого узла дерева. Фрагмент простого примерного дерева событий показан на рис. 5. В этом примере рассматриваются две группы злоумышленников, а также два типа материала, которыми они могут завладеть и с помощью которых изготовить несколько типов устройств. В этом примере рассматриваются четыре возможные цели. На практике



Примечание: На рисунке показана только часть дерева. СЯУ — самодельное ядерное устройство; РДУ — радиологическое диспергирующее устройство; РОУ — радиационное облучающее устройство.

Рис. 5. Пример дерева событий для разработки сценариев рисков.

количество возможных целей может быть намного больше четырех или же цели могут быть описаны как более общие категории или типы целей, а не как конкретные здания или события.

5.27. Следующим шагом является оценка вероятности каждого пути движения по дереву. В этом примере объединение всех возможностей для всех узлов пути приведет к построению 48 отдельных сценариев, и компетентному органу необходимо рассчитать вероятность каждого выбора в каждом узле, чтобы можно было рассчитать вероятность каждого из сценариев.

5.28. Для наглядности показанная древовидная структура специально сделана простой, и на ней не отображены все моменты, связанные с выполнением вероятностной оценки риска. На практике оценка вероятностей может зависеть от других узлов, и может потребоваться дополнительное моделирование или расчет для получения значений вероятностей в узлах с большим количеством вариантов. Данное дерево представляет собой пример того, как можно составить полный набор сценариев при помощи дерева событий. Тщательно построенное дерево позволяет идентифицировать весь круг вероятных сценариев и дать уверенность в том, что результаты охватывают все существенные риски потенциальных событий, связанных физической ядерной безопасностью.

Оценка вероятности сценариев риска

5.29. Ключевым фактором в понимании риска является расчет вероятности различных типов потенциальных событий, связанных с физической ядерной безопасностью — процесс, которому изначально присуща неопределенность. В данном подразделе описаны общие подходы к оценке вероятности, их соответствующие преимущества и недостатки, а также ресурсы, необходимые для проведения соответствующего анализа. Кроме того, проводится сравнение между абсолютными оценками и относительными оценками. Основные соображения сводятся к следующему:

- a) вероятности часто определяются количественно, с тем чтобы их можно было использовать при оценке риска, когда риск зависит от вероятности того, что будет предпринята попытка совершения преступного или преднамеренного несанкционированного действия с ядерным материалом или другим радиоактивным материалом, и от вероятности того, что эта попытка будет успешной (как и последствия);

- b) оценка вероятности изначально имеет неопределенный характер, и поэтому важно оценить не только вероятность, но и степень неопределенности оцениваемой вероятности. Это может быть описано как погрешность оценки (т.е. \pm абсолютная или пропорциональная величина), распределение вероятностей или при помощи слов, обозначающих приблизительные величины;
- c) вероятность может быть оценена как абсолютная вероятность или частота. Однако этот подход часто бывает очень сложен и может не потребоваться при оценке альтернатив на основе оценки риска. Относительная вероятность (т.е. какой из набора сценариев более вероятен и насколько) может быть оценена с большей легкостью, и ее может быть достаточно, если только вероятность этих угроз не потребует сравнить с другими опасностями.

5.30. Один из подходов к оценке вероятности состоит в том, чтобы запросить значения вероятности у соответствующих экспертов. Такой подход позволяет использовать при оценке риска экспертные ресурсы и знания, имеющиеся в государстве, а также проводить ее с учетом национальных особенностей и конкретных сценариев. Однако общение с экспертами может занять очень много времени и натолкнуться на предвзятое отношение ко многим структурным вопросам, если не проводить его с большой осторожностью. Методы, позволяющие избежать этой предвзятости или смягчить ее последствия, описаны в публикации Серии норм безопасности МАГАТЭ, № RS-G-1.9 «Категоризация радиоактивных источников» [18].

5.31. В качестве альтернативы для получения оценок вероятности могут быть разработаны модели. Модели могут охватывать широкий диапазон возможных сценариев и могут быть более гибкими и подходящими для анализа большего числа альтернативных событий. Некоторыми примерами типов моделирования, часто используемых для таких целей, являются деревья событий, деревья отказов и модели теории игр. Полный обзор подходов к моделированию можно найти в [19].

Анализ неопределенности

5.32. При проведении оценок рисков всякий раз приходится иметь дело с неопределенными данными и заключениями, ограниченной способностью прогнозировать или моделировать реальные события, а также

с неопределенными или неоднозначными результатами. Каждый из этих аспектов проблемы неопределенности следует решать с помощью методов, описанных ниже.

- a) Неопределенности в исходных данных для оценки рисков, полученных от экспертов, следует идентифицировать как часть процесса сбора данных или моделирования. Неопределенность обычно описывается распределением возможных значений. Соответствующим экспертам может быть предложено дать оценку нескольких точек распределения (например, среднего значения и крайних значений по обе стороны от среднего, часто 5-го и 95-го перцентиля), и их можно интерпретировать с учетом понимания того, как распределения могут быть искаженными или необъективными. В случае моделирования для получения распределений оценок исходных данных для оценки рисков можно использовать статистические методы.
- b) Неопределенность в исходных данных следует учитывать в течение всего процесса расчета рисков наряду с другими неопределенностями, связанными с этими расчетами. Поскольку прямой расчет распределений для множественных неопределенностей в множественных параметрах быстро становится математически невозможным, для оценки распределений неопределенностей в результатах часто используются другие методы, такие как выборка методом Монте-Карло [20].
- c) Важно донести до лиц, принимающих решения, мысль о неопределенности исходных данных и расчетов в рамках оценки риска и, следовательно, результатов. Когда результаты представляются в числовом виде (например, риски), оценки должны включать указание диапазона, а не просто одно число, а в отчетах о результатах следует избегать вводящих в заблуждение указаний на точность (например, приведения неопределенных результатов к нескольким значащим цифрам).

5.33. Анализ неопределенностей важен, поскольку он служит аргументированным доказательством точности результатов оценки риска как основы для принятия решений. Наличие подтвержденных и проверенных моделей, учитывающих неопределенность, особенно когда вопросы сложны или противоречивы, помогает гарантировать, что решения будут основаны на наилучшей доступной информации.

6. ПРИМЕНЕНИЕ РИСК-ОРИЕНТИРОВАННОГО ПОДХОДА

6.1. Потенциальные последствия события, связанного с физической ядерной безопасностью, могут быть катастрофическими, и государствам следует предпринимать все надлежащие шаги для их предотвращения. Однако ресурсы государства не безграничны, и поэтому государству следует пользоваться методами определения того, какие меры физической ядерной безопасности могут быть наиболее эффективными для снижения риска. Подспорьем для государств в деле оценки возможных вариантов и определения приоритетности мер физической ядерной безопасности может служить риск-ориентированный подход.

6.2. Риск-ориентированный подход — это итеративный процесс, который позволяет: идентифицировать и оценить риски; разработать, оценить, выбрать и внедрить меры по снижению рисков; контролировать



РИС. 6. Пример применения риск-ориентированного подхода при внедрении систем и мер физической ядерной безопасности.

эффективность введенных мер; вносить коррективы по мере необходимости [7]. Риск-ориентированный подход может быть использован как основа для эффективных усилий по минимизации рисков, включающих предотвращение, обнаружение, реагирование, смягчение последствий и восстановление. Он подкрепляет принятие решений по широкому спектру вопросов, включая: стратегическое планирование; выработку политики; формирование бюджета; определение приоритетов в НИОКР; планирование оперативных мероприятий по обеспечению физической ядерной безопасности.

6.3. Целью итеративного риск-ориентированного подхода должно быть постоянное совершенствование и усиление систем и мер физической ядерной безопасности государства с течением времени. Пример такого подхода проиллюстрирован на рис. 6. Пять основных этапов, показанных на рисунке, описаны в нижеследующих пунктах.

6.4. Цикл повторяется на периодической основе (в связи с необходимостью принятия решений или существенным изменением обстоятельств) для улучшения анализа и результатов, а также эффективности систем и мер физической ядерной безопасности. Для достижения целей государства на протяжении всего процесса важно поддерживать связь и проводить консультации между внутренними и внешними заинтересованными сторонами.

6.5. Оценка угроз, будучи инкорпорирована в риск-ориентированный подход как составной элемент оценки рисков, также играет важную роль в идентификации рисков. Она также важна при оценке альтернативных стратегий или систем и мер физической ядерной безопасности (поскольку можно ожидать, что злоумышленник адаптируется к изменениям в применяемых мерах), а также при мониторинге тенденций в изменении угроз и эффективности систем и мер физической ядерной безопасности.

СОЗДАНИЕ УСЛОВИЙ

6.6. На этом этапе уполномоченные компетентные органы определяют, какими типами рисков будут управлять, кто несет ответственность за управление ими, какие решения зависят от информации о рисках (и от какого типа информации) и какие стороны заинтересованы в применении риск-ориентированного подхода. Кроме того, определяются ресурсы для внедрения риск-ориентированного подхода, включая необходимый

бюджет, персонал и организационную структуру. Налаживаются процессы коммуникации между заинтересованными сторонами, и проводится первоначальное обследование функций и мероприятий, связанных с физической ядерной безопасностью.

ОЦЕНКА УГРОЗ И РИСКОВ

6.7. На этом этапе уполномоченный компетентный орган оценивает риски с учетом текущей политики, систем и мер физической ядерной безопасности. В рамках этого этапа уполномоченный компетентный орган оценивает угрозу, уязвимость и последствия возможных действий, связанных с физической ядерной безопасностью, со стороны различных злоумышленников. Методика оценки должна быть согласована с типом принимаемого решения, объемом и качеством имеющихся данных, а также с уровнем и типом имеющихся ресурсов. Методы могут варьироваться от простого кабинетного учения с участием экспертов в соответствующей области до подробных расчетов рисков. Независимо от выбранного метода, важно поддерживать прозрачность в отношении используемой методологии, чтобы у лиц, принимающих решения, не возникало сомнений в достоверности процесса и данных.

ОПРЕДЕЛЕНИЕ АЛЬТЕРНАТИВНЫХ СИСТЕМ И МЕР ФИЗИЧЕСКОЙ ЯДЕРНОЙ БЕЗОПАСНОСТИ

6.8. Используя результаты оценки рисков, компетентные органы, ответственные за внедрение систем и мер физической ядерной безопасности, должны иметь возможность определить, что может быть улучшено для более эффективного реагирования на высокоприоритетные риски преступных или преднамеренных несанкционированных действий с ядерным и другим радиоактивным материалом, находящимся вне регулирующего контроля. К примерам альтернативных мер физической ядерной безопасности может относиться принятие дополнительных мер безопасности или усиление средств защиты регулируемых установок и видов деятельности, усиление пограничного контроля или повышение осведомленности правоохранительных органов, а также введение новых протоколов и регламентов для защиты конкретных целей. При определении, установлении приоритетности и проектировании систем и мер физической ядерной безопасности следует учитывать концепцию глубокоэшелонированной защиты.

6.9. Уполномоченные компетентные органы могут использовать следующие три общих подхода к определению и оценке альтернативных мер: анализ недоработок, анализ затрат и выгод и анализ национальных возможностей.

Анализ недоработок

6.10. Недоработка имеет место тогда, когда отсутствуют достаточные возможности для устранения реальной угрозы. Анализ недоработок предполагает выявление элементов или функций систем физической ядерной безопасности и мер, считающихся необходимыми в свете оценки угроз, которых не существует, которые не выполняются либо которые не позволяют устранить соответствующие угрозы. Недоработки часто выявляются путем изучения угроз, которые приводят к наивысшим рискам, и определения возможностей для нейтрализации этих угроз за счет увеличения объема ресурсов, изменения операций или уменьшения уязвимостей.

Анализ затрат и выгод

6.11. Анализ затрат и выгод позволяет сравнить стоимость мер физической ядерной безопасности с той выгодой, которую они приносят (снижение риска). При этом анализе следует учитывать затраты на принятие мер в течение всего жизненного цикла, что может включать затраты на оборудование, установку, эксплуатацию, техническое обслуживание, людские ресурсы и обучение, а также на модернизацию или вывод из эксплуатации. Снижение риска обычно пересчитывается в денежный эквивалент, что позволяет сравнить затраты на принятие мер. Это способствует применению дифференцированного подхода к совершенствованию систем и мер физической ядерной безопасности. Некоторые «издержки» от принятия мер также могут носить неденежный характер — например, изменения в планах и процедурах и перераспределение активов.

Анализ национальных возможностей

6.12. Анализ национальных возможностей предполагает оценку всего комплекса систем и мер физической ядерной безопасности как интегрированной системы реагирования на угрозы. Такой подход часто используется, когда необходимо смоделировать поведение злоумышленников, намерения которых могут динамично меняться в зависимости от конкретно применяемых мер физической ядерной

безопасности. Например, усиление охраны одного стратегического объекта может повысить вероятность нападения злоумышленника на другой объект. Усиление охраны обоих объектов может привести к тому, что злоумышленник решит применить иной тип атаки. Таким образом, реальная ценность повышения физической безопасности одного объекта может быть оценена только с точки зрения того, как меняется (или нет) физическая безопасность других объектов. Простейший подход к анализу национальных возможностей заключается в оценке риска для нескольких альтернативных комплексов систем и мер и определении ценности конкретного типа мер на основе того, как часто они включаются в наиболее эффективные комплексы.

6.13. При оценке влияния систем и мер на риск важно помнить, что злоумышленники могут менять тактику в ответ на применение новых или дополнительных мер физической ядерной безопасности. Таким образом, поскольку злоумышленники просто меняют тактику, общее снижение риска, как правило, меньше по сравнению с ситуацией, в которой угроза статична (т.е. злоумышленник рассматривает только один тип нападения на одну цель). Иногда усиление безопасности в одном месте может побудить злоумышленников перейти к другому сценарию, который был бы более успешным даже при прежних системах и мерах. В таком случае в результате усиления безопасности в некоторых местах на самом деле может произойти увеличение общего риска. Понимание наклонностей злоумышленников и вероятных мер реагирования может гарантировать, что дополнительная защита приведет к желаемому снижению риска.

6.14. Поскольку ответственность за все системы и меры физической ядерной безопасности в государстве часто распределяется между рядом различных компетентных органов, важно координировать использование ресурсов и подходы к снижению риска. Надлежащая координация поможет обеспечить своевременное внедрение одним компетентным органом систем и мер, способствующих эффективному выполнению обязанностей другого компетентного органа.

ВНЕДРЕНИЕ СИСТЕМ И МЕР ФИЗИЧЕСКОЙ ЯДЕРНОЙ БЕЗОПАСНОСТИ

6.15. Системы и меры физической ядерной безопасности должны быть внедрены (спроектированы, введены в действие и поддерживаться в надлежащем состоянии) после выбора государством направления действий.

Для того чтобы проекты исполнялись в соответствии с техническими требованиями, в срок и в рамках выделенного бюджета, процесс внедрения должен базироваться на надлежащей практике менеджмента.

6.16. После того как системы и меры физической ядерной безопасности будут выбраны и спроектированы, начинается их внедрение, которое обычно включает в себя разработку, приобретение, установку, эксплуатацию и обслуживание технических средств и поддержание их в работоспособном состоянии [11]. В процессе внедрения следует принимать во внимание требования по защите чувствительной информации и чувствительных информационных активов, связанных с системами и мерами физической ядерной безопасности.

6.17. Риск-ориентированный подход к определению приоритетности и внедрению отличается от подхода, основанного на учете рисков, при котором риск является главным и решающим фактором установления приоритетов. Существует множество факторов, которые следует учитывать при определении приоритетности систем и мер физической ядерной безопасности (например, бюджетные факторы, политические факторы, осуществимость и приемлемость мер, эффективность, а также прочие затраты, обусловленные этими мерами). Риск является одним из факторов, лежащих в основе общего определения приоритетов, и должен учитываться лицами, принимающими решения, в сочетании с этими прочими факторами.

МЕНЕДЖМЕНТ РИСКОВ

6.18. Развертывание и внедрение систем и мер физической ядерной безопасности не должно быть разовым действием. Эти системы и меры должны эксплуатироваться, поддерживаться в рабочем состоянии и быть устойчивыми, а также модернизироваться или адаптироваться по мере изменения ситуации. Системы и меры следует тестировать с целью убедиться в том, что они функционируют в соответствии с проектом. На этом этапе следует провести повторную оценку эффективности систем и мер физической ядерной безопасности на практике (т.е. действительно ли они работают так, как предполагается). Кроме того, следует постоянно отслеживать угрозы и уязвимости для выявления изменений, влияющих на угрозу, таких как информация о новых злоумышленниках, изменение целей или возможностей злоумышленников, разработка новых систем и мер физической ядерной безопасности и другие факторы. Результаты

такого мониторинга следует использовать для актуализации информации об анализе обстоятельств и рисков при следующем повторении цикла риск-ориентированного подхода.

Оценка эффективности

6.19. Показатели эффективности предназначены для измерения того, насколько хорошо системы и меры физической ядерной безопасности справляются с задачами предупреждения, обнаружения и реагирования на угрозы, связанные с ядерным и другим радиоактивным материалом, находящимся вне регулирующего контроля. На практике рассчитать показатели, которые имели бы практическую ценность, чрезвычайно сложно, поскольку попытки хищения материалов или совершения действий, имеющих последствия для физической ядерной безопасности, крайне редки. В отсутствие фактического опыта, полученного на основе реальных событий, следует разрабатывать модели или косвенные показатели.

6.20. В ходе учебных мероприятий, учитывающих все необходимые ресурсы для функционирования систем и мер физической ядерной безопасности, может быть выявлена эффективность мер и получена информация об общей эффективности внедренной системы. Как правило, для оценки эффективности систем и мер физической ядерной безопасности может использоваться комбинация результатов учений, других показателей эффективности (таких как среднее время между отказами) и моделей.

Анализ тенденций

6.21. Помимо расчета эффективности систем и мер физической ядерной безопасности с точки зрения нейтрализации ранее выявленных угроз, для отражения изменений в возможностях важно актуализировать оценку угроз. Для анализа изменений можно задаться вопросами, указанными ниже.

- Произошли ли изменения в поведении известных злоумышленников? Отмечены ли у них дополнительные технические возможности или экспертные знания? Наладили ли они новые контакты с другими негосударственными субъектами?
- Появились ли новые злоумышленники, которые могут планировать действия, имеющие последствия для физической ядерной безопасности?

- Проявляли ли злоумышленники дополнительный интерес к государству как к цели, безопасному убежищу или источнику ядерного материала или другого радиоактивного материала?
- Отмечены ли заметные изменения в коммерческих перевозках или контрабандных перевозках через территорию государства? Требуется ли увеличение объема перевозок дополнительного изучения?
- Были ли внесены крупные изменения в системы и меры физической ядерной безопасности? Появились ли новые объекты, предназначенные для хранения или использования ядерного или другого радиоактивного материала, и не изменились ли существенно объемы или типы такого материала?

6.22. Выявление изменений в угрозах, а также в государственных системах и мерах физической ядерной безопасности — важный шаг для определения того, когда следует провести актуализацию риск-ориентированного подхода или инициировать новый цикл его применения. Этот цикл следует периодически повторять в координации с процессами принятия решений. Кроме того, когда происходят значительные изменения в государственных системах обнаружения событий, связанных с физической ядерной безопасностью, и реагирования на них [10, 11] либо в самой угрозе, должна быть пересмотрена и актуализирована оценка риска и повторен цикл применения риск-ориентированного подхода.

Приложение I

БЛОК-СХЕМА ОЦЕНКИ УГРОЗ И ПРИМЕНЕНИЯ РИСК-ОРИЕНТИРОВАННОГО ПОДХОДА

I.1. На блок-схеме в настоящем приложении (см. рис. 7) показан полный цикл применения риск-ориентированного подхода. Все важные этапы, описанные в данной публикации, сведены в единый общий процесс.

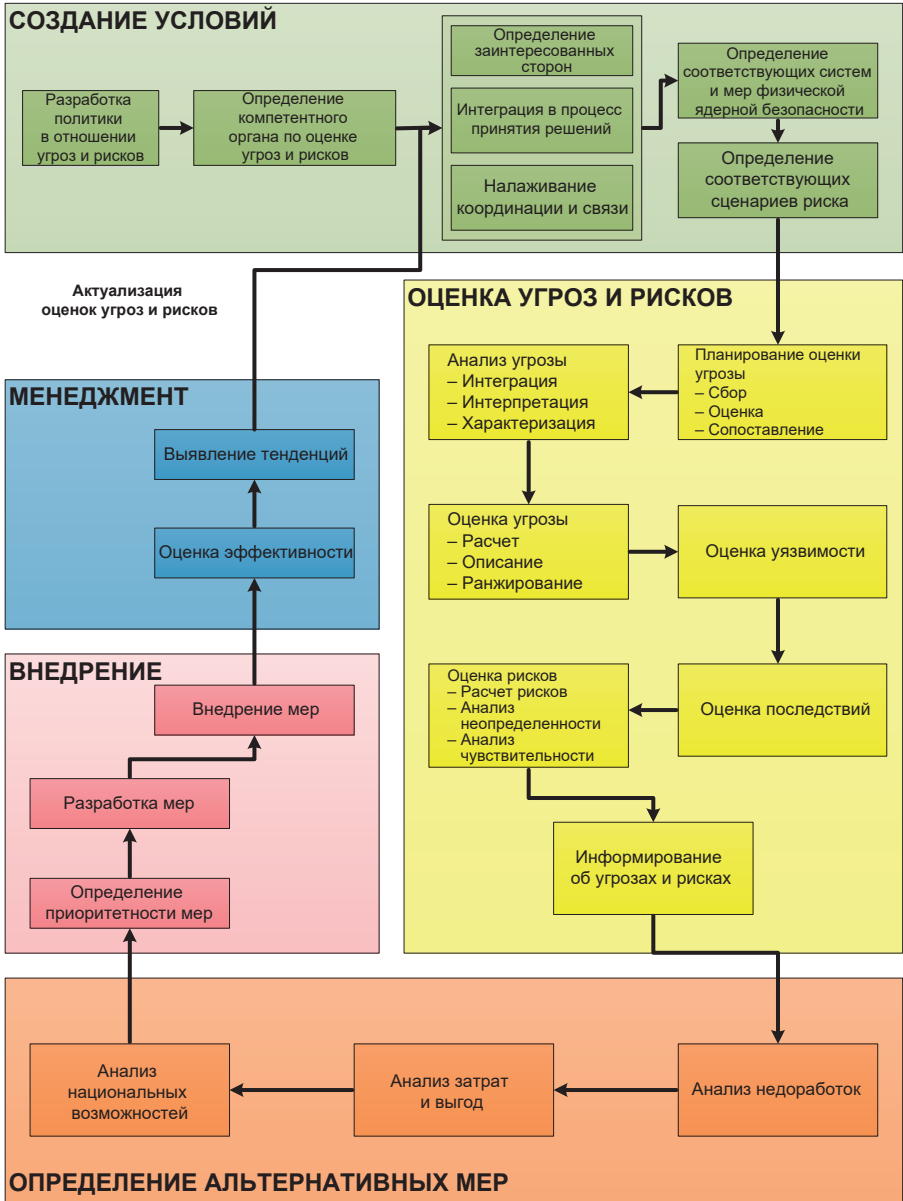


РИС. 7. Блок-схема оценки угроз и применения риск-ориентированного подхода.

Приложение II

ПРИМЕР ОЦЕНКИ УГРОЗЫ

КОНТЕКСТ ОЦЕНКИ

II.1. Для краткости в этом примере опущены все рассуждения, процессы и аналитические выкладки, лежащие в основе оценок. Показаны примерные результаты процессов и то, как результаты могут быть представлены заинтересованным сторонам.

II.2. В приложениях II–IV в качестве примера используется вымышленное государство, именуемое «условным государством». В условном государстве есть атомная электростанция и исследовательский реактор, но отсутствует полный ядерный топливный цикл. В условном государстве также есть больницы, в которых хранятся и используются радиоактивные материалы и источники, и другие отрасли (например, строительная), в которых имеется значительное количество радиоактивных источников, лицензированных регулирующим органом условного государства.

II.3. Ответственность за регулирование ядерного материала и другого радиоактивного материала на соответствующих установках и в рамках соответствующей деятельности, а также за обнаружение событий, связанных с физической ядерной безопасностью и реагирование на них, лежит на нескольких компетентных органах условного государства. Все эти органы сотрудничают и взаимодействуют с компетентным органом, ответственным за оценку угроз и рисков, в целях применения риск-ориентированного подхода к мерам по обеспечению физической ядерной безопасности ядерного и другого радиоактивного материала, находящегося вне регулирующего контроля. Кроме того, компетентный орган условного государства отмечает известные недоработки и учитывает актуальность и своевременность информации и разведывательных данных, используемых для проведения оценки угроз.

II.4. Существует несколько процессов принятия решений, которые могут базироваться на риск-ориентированном подходе, помогающем определить приоритеты при использовании ограниченных ресурсов. Условное государство рассчитывает на то, что процесс менеджмента рисков поможет ему сэкономить ресурсы.

ИДЕНТИФИКАЦИЯ МАТЕРИАЛА И ЗЛОУМЫШЛЕННИКОВ

II.5. Компетентный орган условного государства проводит процесс идентификации угроз, в котором учитываются злоумышленники, а также ядерный и другой радиоактивный материал, находящийся вне регулирующего контроля. Анализ инцидентов, зафиксированных в ITDB, показывает, что:

- a) строительные контрольно-измерительные приборы, содержащие радиоактивный материал, были похищены на территории условного государства и не были возвращены;
- b) в соседнем государстве к западу от условного государства зарегистрировано в три раза больше инцидентов, чем в государствах к северу, востоку и югу;
- c) ядерный материал, пригодный для изготовления СЯУ, никогда не терялся, не пропал и не похищался в государстве или в соседних государствах, однако нельзя полностью исключать возможность его приобретения в этих государствах или в другом государстве.

II.6. Компетентный орган проводит оценку и заключает, что существуют три класса потенциальных злоумышленников, которых следует учитывать при определении угрозы и риска:

- a) международная группа злоумышленников, которая может либо совершить действие в пределах границ условного государства, либо использовать условное государство в качестве плацдарма для совершения действия против другого государства;
- b) внутренняя группа злоумышленников, которая выступала за свержение нынешнего правительства и совершала другие насильственные действия;
- c) отдельное лицо или небольшая группа лиц с конкретным планом, а также со склонностью к насилию.

II.7. Компетентный орган предоставляет специалистам по анализу угроз информацию о групповых тенденциях, известных планах и целях. Собираются и сопоставляются данные о недавних инцидентах, имеющих отношение к делу (действиях, указывающих на групповые тенденции, либо действиях, связанных с физической ядерной безопасностью).

ИДЕНТИФИКАЦИЯ ЦЕЛЕЙ

П.8. Компетентный орган условного государства, ответственный за оценку угроз и рисков, определяет несколько ключевых потенциальных целей для действий, связанных с ядерным или другим радиоактивным материалом, находящимся вне регулирующего контроля. В качестве основных целей при анализе угроз рассматриваются:

- деловой центр столицы условного государства;
- главный торговый район основного туристического города условного государства;
- несколько важных правительственных зданий, в которых размещены ключевые ведомства условного государства;
- ежегодные торжества по случаю национального праздника.

П.9. Поскольку число идентифицированных целей в условном государстве относительно невелико, они оцениваются индивидуально. Если компетентный орган решит оценить гораздо больше потенциальных целей, то эти цели можно сгруппировать по типам.

ОПРЕДЕЛЕНИЕ ПОСЛЕДСТВИЙ

П.10. Для оценки вероятных последствий ряда потенциальных действий против идентифицированных целей компетентный орган условного государства создает группу экспертов по взрывчатым веществам, радиации и преступным или преднамеренным несанкционированным действиям. Эксперты рассматривают множество переменных, которые могут повлиять на фактический размер последствий, включая количество и тип радиоактивного материала, метеорологические условия в момент совершения действия, характер цели и характеристики самого действия. Затем группа предоставляет расчеты последствий для ряда сценариев, выраженные величинами одного порядка. По каждому сценарию могут быть даны оценки человеческих жертв и экономических убытков (для простоты экономические убытки включают в себя экологические и социальные

последствия). Совокупная стоимость последствий (стоимость) и нормализованный рейтинг последствий могут быть рассчитаны следующим образом:

$$\text{Стоимость} = \text{жертвы} \times \text{номинальная стоимость жертв} + \text{экономические} + \text{экологические} + \text{социальные} \quad (1)$$

$$\text{Нормализованный рейтинг последствий} = 100 \times \frac{\text{Стоимость}}{\text{Макс. (Стоимость)}} \quad (2)$$

II.11. Поскольку целью компетентного органа является установление относительной тяжести последствий для разных сценариев, число жертв может быть умножено на среднюю стоимость в один миллион денежных единиц (для иллюстрации) и прибавлено к экономическим издержкам для получения совокупного показателя затрат. Полученные значения могут быть нормализованы по наибольшему значению, чтобы получить шкалу нормализованного рейтинга последствий от 0 до 100. Таблица последствий, составленная в результате этого анализа, приведена в таблице 4.

ТАБЛИЦА 4. ОТНОСИТЕЛЬНАЯ ТЯЖЕСТЬ ПОСЛЕДСТВИЙ РЕАЛИЗАЦИИ УСЛОВНЫХ СЦЕНАРИЕВ ДЛЯ УСЛОВНОГО ГОСУДАРСТВА

Сценарий	Здоровье человека (число жертв)	Экономические издержки (в миллионах денежных единиц)	Нормализованный рейтинг последствий
СЯУ в столичном городе	20 000	250 000	100
СЯУ в туристическом городе	10 000	100 000	40,74
РДУ в столичном городе	500	500	0,37
РДУ в правительственном здании	20	100	0,04
РДУ на праздновании	2 000	250	0,83
РОУ в туристическом городе	150	10	0,06

ТАБЛИЦА 4. ОТНОСИТЕЛЬНАЯ ТЯЖЕСТЬ ПОСЛЕДСТВИЙ РЕАЛИЗАЦИИ УСЛОВНЫХ СЦЕНАРИЕВ ДЛЯ УСЛОВНОГО ГОСУДАРСТВА (продолжение)

Сценарий	Здоровье человека (число жертв)	Экономические издержки (в миллионах денежных единиц)	Нормализованный рейтинг последствий
РОУ на праздновании	350	50	0,15
РОУ в правительственном здании	15	5	0,01
Акт загрязнения	800	250	0,39

Примечание: Цифры являются условными и не предназначены для использования вне данного примера. СЯУ — самодельное ядерное устройство; РДУ — радиологическое диспергирующее устройство; РОУ — радиационное облучающее устройство.

ОЦЕНКА УГРОЗ

II.12. Компетентный орган условного государства, ответственный за проведение оценки угроз и рисков, координирует усилия различных компетентных органов по составлению описания угроз для трех идентифицированных типов злоумышленников. Экспертам предоставляются данные и карты с информацией об известных или предполагаемых случаях незаконного оборота ядерного материала или другого радиоактивного материала. Затем инциденты разбиваются по типу материала, месту и характеру инцидента, а также по происхождению или законному использованию материала. Соответствующим экспертам также предоставляются информационные сводки, описывающие заявленные цели, недавнюю деятельность и риторику каждой из известных групп, чтобы они могли провести общую оценку и выработать единый подход. В таблице 5 приведен пример такого консенсусного подхода, выработанного экспертами.

ТАБЛИЦА 5. ПРИМЕР ОПИСАТЕЛЬНОГО АНАЛИЗА УГРОЗ
ДЛЯ ТРЕХ ГРУПП ЗЛОУМЫШЛЕННИКОВ

Злоумышленник	Намерение	Возможности
Международная группа	Цель группы — нанести высокий экономический ущерб или вызвать массовые жертвы.	Группа пыталась приобрести или похитить радиоактивный материал, но ее планы были сорваны правоохранительными органами. Группа получила значительные средства в результате преступной деятельности, но в силу правил внутренней безопасности ей было трудно нанять технических экспертов или связаться с лицами, имеющими доступ к радиоактивному материалу.
Местная группа	Цель группы — нанести экономический ущерб правительству условного государства, чтобы добиться территориальной автономии, без массовых жертв, которые вызвали бы возмущение международной общественности.	Группа имеет четкую иерархию, основанную на семейных связях, и занимается извлечением незаконного дохода, например от торговли наркотиками. Ни один из известных членов организации не имеет высшего университетского образования в области физики или инженерии, хотя они продемонстрировали умение изготавливать обычное оружие собственными силами. В прошлом они никогда не пытались приобрести ядерный материал или другой радиоактивный материал.
Одиночный злоумышленник	Одиночный злоумышленник в первую очередь стремится нанести ущерб работодателю и дискредитировать его. Он может довольствоваться причинением серьезного ранения или смерти, но массовые жертвы не являются частью его цели.	Это лицо имеет доступ к ядерному материалу или другому радиоактивному материалу и специальные знания об обращении с ним, но никогда не соорудило полноценное устройство. Таким образом, вероятно совершение только действий, связанных с применением радиационного облучающего устройства или вызывающих ограниченное загрязнение.

II.13. Используя подход, основанный на ранжировании угроз, компетентный орган, ответственный за оценку угроз и рисков, также проводит опрос соответствующих экспертов для ранжирования каждого конкретного сценария в сочетании с типами злоумышленников. При данном подходе оценка делится на несколько подкатегорий. Возможности можно разделить на организационные, технические и финансовые. Намерения можно разделить на идеологию и цель. Вероятность создания устройства можно разделить на такие критерии, как материал, сложность приобретения материала и сложность изготовления устройства. Наконец, уязвимость цели можно разделить на тип цели и время нападения. Каждый из этих критериев или факторов оценивается на основе определенных оценочных шкал (также называемых «метаграммами»), которые устанавливают критерии для каждого рейтинга. Пример оценки использования некоей местной повстанческой группировкой РДУ на ежегодном праздновании показан в таблицах 6–8 и описан в пунктах II.14–II.16.

ТАБЛИЦА 6. ПРИМЕР РАНЖИРОВАНИЯ УГРОЗ НА ОСНОВЕ ВОЗМОЖНОСТЕЙ И НАМЕРЕНИЙ

Рейтинг компонентов оценки угроз	Возможности			Намерение	
	Организа- ционные	Техни- ческие	Финансовые/ логистические	Идеология/ наклонности	Цель/ мотив
Очень высокий					
Высокий					
Средний					
Низкий					
Очень низкий					

ТАБЛИЦА 7. ПРИМЕР РАНЖИРОВАНИЯ УГРОЗ НА ОСНОВЕ МАТЕРИАЛА И УЯЗВИМОСТИ

Рейтинг компонентов оценки угроз	Материал			Уязвимость цели	
	Тип материала	Приобретение	Устройство	Тип цели	Возможность/временные рамки
Очень высокий					
Высокий					
Средний					
Низкий					
Очень низкий					

ТАБЛИЦА 8. ПРИМЕР ОБОБЩЕННОГО РЕЙТИНГА УГРОЗ

Общий рейтинг при оценке угроз
Очень высокий
Высокий
Средний
Низкий
Очень низкий

П.14. Местная группа хорошо организована и финансируется, но не проявляла интереса к ядерному материалу или другому радиоактивному материалу и не демонстрировала осведомленности о нем. Хотя они обычно не стремятся вызвать жертвы среди гражданского населения, у них есть твердое намерение совершить действие, которое повысило бы их престиж и авторитет.

II.15. Интересующий группу радиоактивный материал имеется в условном государстве, но доступ к нему строго контролируется. Однако как только группа завладеет материалом, устройство будет легко сконструировать. Целью является очень уязвимый гражданский объект, но время для достижения максимального эффекта крайне ограничено.

II.16. В целом сочетание факторов для местной группировки, применяющей РДУ на ежегодном праздновании в условном государстве, дает высокий рейтинг угрозы: возможности и намерения оцениваются как высокие, а привлекательность материала и цели оцениваются от высокой до очень высокой. То, как проводится эта оценка, и общий рейтинг угрозы будет зависеть от используемой методологии.

II.17. Аналогичные оценки, выполненные для каждой пары «злоумышленник-сценарий», используются для оценки потенциальных действий. Такое ранжирование лежит в основе расчетов относительной вероятности рассмотренных вариантов событий в области физической ядерной безопасности с использованием ядерного и другого радиоактивного материала, находящегося вне регулирующего контроля. Эта общая оценка будет обоснована подтверждающими данными для оценки по каждому критерию и подтверждена с помощью соответствующей экспертизы.

Приложение III

ПРИМЕР ОЦЕНКИ РИСКА

III.1. В нижеследующем примере демонстрируется использование методологии вероятностной оценки риска путем создания дерева событий для условного государства. Оцениваются значения, необходимые для вероятностных расчетов сценариев данного дерева, и представляются результаты выборочного анализа. Этот пример основан на примере оценки угрозы, приведенном в приложении II, и использует его результаты.

СТРУКТУРА СЦЕНАРИЕВ

III.2. Узлы дерева и все альтернативные варианты каждого узла представлены на рис. 8. На данном дереве отображен минимальный набор типов узлов, необходимых для описания событий в области физической ядерной безопасности, связанных с материалом, находящимся вне регулирующего контроля. Для простоты количество альтернативных путей от каждого узла сведено к минимуму. Вероятность существования каждого из узлов рассматривается как распределение возможностей. Как это обычно бывает с таким деревом событий, вероятность в некоторых узлах зависит от значений в других узлах. Например, существование узла «устройство» зависит от приобретенного материала. Для некоторых государств может оказаться необходимым или желательным ввести дополнительные зависимости в оценку рисков.

III.3. Конкретный сценарий, созданный деревом событий, показан линией, проходящей через дерево. Например, одним из сценариев может быть то, что местная группа, получив мощный источник излучения, решает использовать его в качестве РДУ для совершения нападения во время ежегодного празднования (сценарий 2 на рисунке обозначен линией оранжевого цвета). Показанное дерево, будучи полностью развернутым, может содержать до 120 сценариев (три возможных злоумышленника × два типа материала × четыре типа устройств × пять потенциальных целей). Однако после удаления нереалистичных комбинаций (например, мощный источник гамма-излучения непригоден для изготовления СЯУ, и СЯУ не может считаться подходящим средством для загрязнения пищевых продуктов и воды) общее количество логичных сценариев, остающихся в модели риска, сократится до 36. Оценка риска выполняется путем расчета вероятности каждого из сценариев и расчета последствий

возможной реализации этого сценария. Последствия были рассчитаны ранее в приложении II, и соответствующие расчеты приведены в таблице 4 этого приложения. Для целей оценки риска при расчетах последствий используется нормализованный рейтинг последствий.

РАСЧЕТ ВЕРОЯТНОСТИ

III.4. Расчет вероятности сценариев выполняется путем расчета вероятности каждого из элементов сценария (с учетом зависимостей, где это применимо). Для условного государства некоторые примерные расчеты вероятности приведены на рис. 8. Расчетные вероятности, представленные на рисунке, являются относительными вероятностями для каждого уровня дерева. Другими словами, значение вероятности отдельно взятой альтернативы на одном уровне дерева событий определяет относительную вероятность альтернатив уровнем ниже. Расчеты, подобные этим, могут быть получены от соответствующих экспертов, и при полной оценке риска следует учитывать распределение неопределенностей. Важно отметить, что значения вероятности присваиваются только возможным ветвям дерева событий. На рис. 8 показано, что для определения вероятностей всех сценариев достаточно выполнить 23 расчета.

ОЦЕНКА РИСКА

III.5. Риск сценария оценивается путем расчета вероятности реализации сценария и умножения ее на значение рейтинга последствий (значения нормализованного рейтинга последствий указаны в таблице 4 приложения II). В этом примере для автоматического выполнения всех расширений сценария и вычислений можно использовать электронную таблицу. Вместе с тем пример, приведенный в таблице 9, иллюстрирует расчет для двух сценариев, выделенных на рис. 8.

ТАБЛИЦА 9. ПРИМЕРНЫЕ РАСЧЕТЫ РИСКА ДЛЯ ДВУХ СЦЕНАРИЕВ

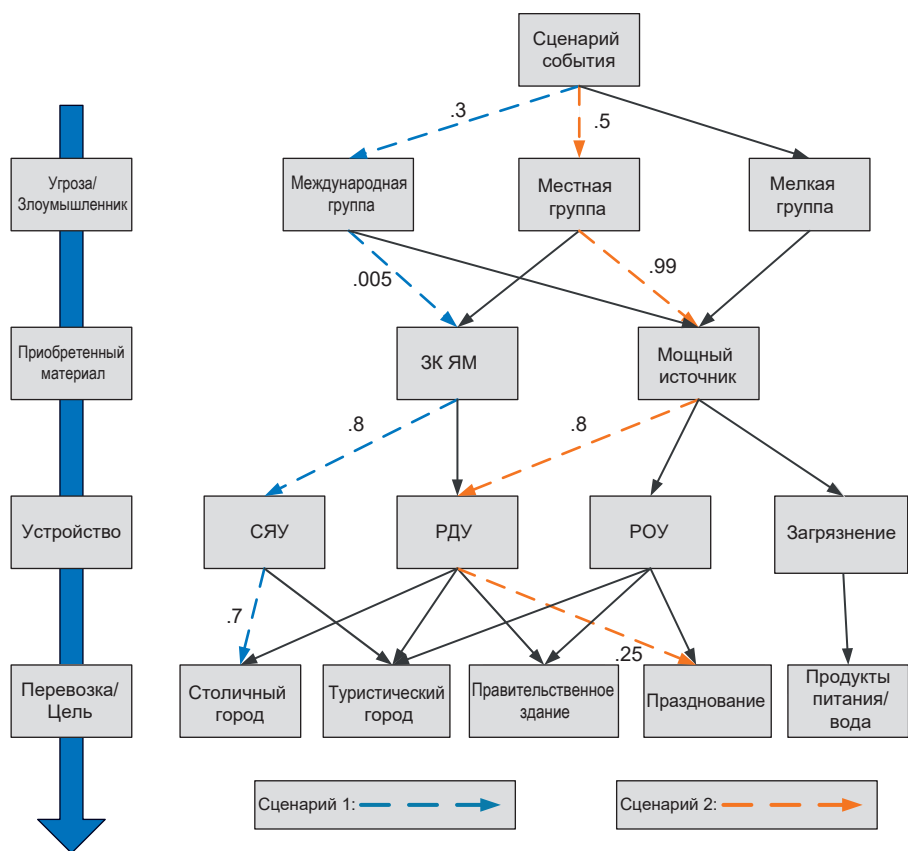
Сценарий 1. Международная группа получает ЗК ЯМ и применяет СЯУ в столичном городе		
Вероятность =	$0,3 \times 0,005 \times 0,8 \times 0,7$	= 0,00084
Риск сценария ^а =	$0,00084 \times 100$	= 0,084
Сценарий 2. Местная группа получает мощный радиоактивный источник и применяет РДУ на праздновании		
Вероятность =	$0,5 \times 0,99 \times 0,8 \times 0,25$	= 0,099
Риск сценария =	$0,099 \times 0,83$	= 0,082

Примечание: СЯУ — самодельное ядерное устройство; РДУ — радиологическое диспергирующее устройство; ЗК ЯМ — значимое количество ядерного материала.

^а Риск сценария = вероятность × нормализованный рейтинг последствий.
См. таблицу 4 приложения II.

III.6. Сценарий 1 предполагает применение СЯУ в столичном городе. Сценарий 2 предполагает применение РДУ на ежегодном праздновании. Сценарий 2 оценивается как примерно в 100 раз более вероятный, чем сценарий 1 (0,099 по сравнению с 0,00084), но размер последствий сценария 1 почти в 100 раз больше (100 по сравнению с 0,83). Разница в относительных вероятностях уравнивается разницей в последствиях, так что оба сценария несут в себе примерно одинаковый риск. Таким образом, значения риска используются для сравнения сценариев, а не как некое абсолютное значение риска.

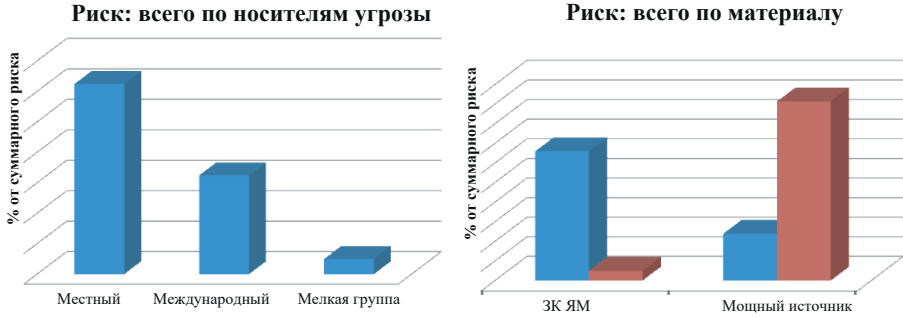
III.7. Описания сценариев 1 и 2 содержат подробную информацию о расчете двух конкретных сценариев. В общей оценке рисков существует гораздо больше сценариев, и часто рассмотреть каждый сценарий в отдельности не представляется возможным. Вместо этого сценарии группируются по характеристикам (например, один и тот же злоумышленник или один и тот же материал). Представить риски графически, чтобы это имело практическую ценность, можно, если взять определенный аспект риска (например, злоумышленника или цель) и проанализировать сумму рисков по всем сценариям, связанным с конкретной группой угроз или



Примечание: Согласно дереву событий, приведенному в примере, могут быть приобретены два типа ядерных материалов: мощный источник (источник категории 1 [18]) и значимое количество ядерного материала (ЗК ЯМ). СЯУ — самодельное ядерное устройство; РДУ — радиологическое диспергирующее устройство; РОУ — радиационное облучающее устройство.

РИС. 8. Дерево события с выделением двух примерных сценариев.

целью. Два таких изображения, относящихся к данному примеру, показаны на рис. 9. Следует отметить, что в данном примере отдельные сценарии для СЯУ и РДУ имеют приблизительно равный риск, но после учета всех сценариев риск СЯУ будет намного больше, чем риск РДУ.



Примечание: Голубые столбцы обозначают риск. Коричневые столбцы обозначают вероятность реализации сценария с использованием указанного материала. ЗК ЯМ — значимое количество ядерного материала.

РИС. 9. Два примера графического изображения риска.

III.8. На левом рисунке показаны риски, исходящие от местных, международных и мелких групп злоумышленников. В данном случае наибольший риск несет в себе местная группа, наименьший — мелкие группы. На правом рисунке показана разница между риском и вероятностью для двух типов материала при оценке риска. Синие столбцы в каждой паре представляют собой риск. На диаграмме ЗК ЯМ представляет больший риск. Коричневые столбцы в каждой паре — это вероятность реализации сценариев с использованием указанного материала. Сценарий с мощным источником намного более вероятен. Разница между риском и вероятностью учитывается при помощи последствий. Мощные источники можно использовать в других устройствах, но СЯУ должны содержать ядерный материал. Однако СЯУ потенциально могут вызвать гораздо более серьезные последствия (как явствует из этой условной оценки), так что разница в последствиях перевешивает разницу в вероятности. Оценка риска в значительной мере основывается на понимании этой взаимосвязи между вероятностью, последствиями и риском.

III.9. Другой ключевой фактор понимания риска связан с отображением неопределенности в расчетах. На рис. 10 показан пример диаграммы неопределенности риска для разных потенциальных мест расположения цели. В дополнение к среднему риску (представленному столбцом для каждой цели), на диаграмме линией показана неопределенность в оценке риска для каждой цели. Верхний и нижний концы линии для каждой цели представляют, соответственно, 95-й и 5-й процентиля распределения неопределенности, и они часто рассчитываются на основе неопределенных

вероятностных распределений при помощи методов Монте-Карло. На данной диаграмме аналитик может обнаружить серьезные различия в риске. Например, очевидно, что столица подвержена большему риску, чем любая другая цель, однако туристический город и ежегодное празднование имеют перекрывающиеся распределения неопределенности.

III.10. Таким образом, при оценке риска крайне важно понимать, как неопределенность влияет на результаты. В некоторых оценках с большими неопределенностями может быть трудно провести четкое различие между рисками с более высокими и более низкими средними значениями. Во многих случаях могут быть четко различимы только выбросы (самые высокие и самые низкие значения риска), а между ними будет находиться множество рисков схожей величины. При использовании только средних значений риска оценка риска кажется более точной, чем это оправдано, что может вводить в заблуждение. Данные диаграммы могут помочь специалисту по анализу риска выполнить оценку риска и проинформировать о ней лиц, принимающих решения.

Риск: всего по целям

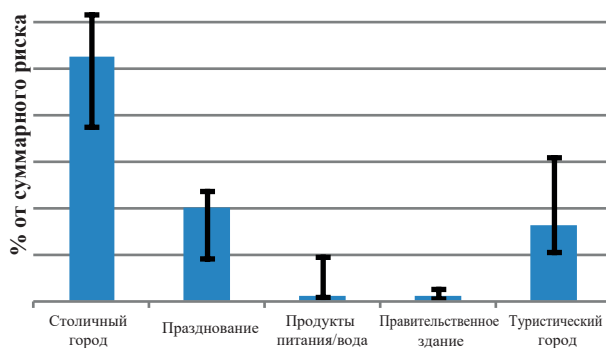


РИС. 10. Пример диаграммы риска с указанием диапазонов неопределенности.

Приложение IV

ПРИМЕР ПРИМЕНЕНИЯ РИСК-ОРИЕНТИРОВАННОГО ПОДХОДА

IV.1. В нижеследующем примере демонстрируется применение результатов оценок угроз и рисков в рамках риск-ориентированного подхода с использованием как исходных, так и выходных данных (описанных в приложениях II и III соответственно). Данное приложение посвящено второй половине цикла применения риск-ориентированного подхода: анализу и выбору альтернатив, внедрению выбранных систем и мер, а также текущему управлению программой, которое предполагает актуализацию оценок угроз и проведение оценок эффективности внедренных систем и мер физической ядерной безопасности.

ИДЕНТИФИКАЦИЯ, ОПРЕДЕЛЕНИЕ ПРИОРИТЕТНОСТИ И ВНЕДРЕНИЕ

IV.2. После оценки рисков, описанной в приложении III, соответствующие компетентные органы (компетентный орган, ответственный за оценку угроз и рисков, и компетентные органы, ответственные за охрану различных объектов) определяют потенциальные системы и меры, которые могут быть применены для снижения риска совершения действия, имеющего последствия для физической ядерной безопасности. В одних случаях может быть оценена только одна мера; в других случаях может быть дана оценка множеству альтернативных мер. В таблице 10 перечислены потенциальные системы и меры, подлежащие оценке. Для каждой системы или меры компетентные органы оценивают, насколько может быть снижена вероятность события, связанного с физической ядерной безопасностью, благодаря применению этой системы или меры, а также затраты на внедрение этой системы или меры.

IV.3. Такие системы и меры оцениваются как по отдельности, так и в сочетании друг с другом, чтобы определить степень снижения рисков для каждого уровня расходов. График этого анализа затрат и выгод (где выгодой считается снижение риска) показан на рис. 11. Каждая точка представляет собой один вариант обеспечения безопасности (т.е. один возможный набор систем и мер) в каждом из мест расположения цели, показанных в таблице 10. Квадратики представляют собой наборы выбранных опций, которые могут реализовываться один за другим для оптимального повышения физической

безопасности. Варианты безопасности, обеспечивающие наименьший риск в расчете на единицу затрат, находятся на синей линии (обозначены как «оптимальный вариант обеспечения безопасности»).

ТАБЛИЦА 10. ПОТЕНЦИАЛЬНЫЕ СИСТЕМЫ И МЕРЫ ФИЗИЧЕСКОЙ ЯДЕРНОЙ БЕЗОПАСНОСТИ ДЛЯ УСЛОВНОГО ГОСУДАРСТВА

Местонахождение цели	Вариант систем или мер	Описание
Столичный город	Исходный вариант	Возможности, имеющиеся в столичном городе на данный момент
	Добавлена полиция	Увеличено число полицейских, осуществляющих патрулирование в столичном городе
	Добавлены датчики	Приобретение и установка детекторов излучений в столичном городе
Туристический город	Исходный вариант	Возможности, имеющиеся в туристическом городе на данный момент
	Усилены процедуры	Организация обучения и создание технической базы для того, чтобы сотрудники полиции туристического города могли распознавать и идентифицировать угрозы физической ядерной безопасности
Правительственное здание	Исходный вариант	Возможности, имеющиеся в правительственном здании на данный момент
	Усилена физическая защита	Улучшены физические барьеры (замки, системы пропуска, двери и окна, а также бетонные ограждения), защищающие здание
	Система охраны	Установлена система охраны с сигнализацией на дверях и окнах, некоторыми датчиками излучений и камерами видеонаблюдения

ТАБЛИЦА 10. ПОТЕНЦИАЛЬНЫЕ СИСТЕМЫ И МЕРЫ ФИЗИЧЕСКОЙ ЯДЕРНОЙ БЕЗОПАСНОСТИ ДЛЯ УСЛОВНОГО ГОСУДАРСТВА (продолжение)

Местонахождение цели	Вариант систем или мер	Описание
Национальный праздник	Исходный вариант	Возможности по обеспечению защиты на национальном празднике, имеющиеся на данный момент
	Охрана периметра	Усиление охраны периметра во время проведения национального праздника путем установки барьеров и пропуска людей на территорию через четко обозначенные проходы, где возможно принятие мер обнаружения
	Усилены процедуры	Проведение информационных брифингов и предоставление сотрудникам полиции возможности обратной связи для распознавания и идентификации угроз физической ядерной безопасности
	Усилено патрулирование	Увеличение числа и снижение предсказуемости действий групп сотрудников охраны, осуществляющих патрулирование во время проведения национального праздника
Продукты питания и вода	Исходный вариант	Возможности, имеющиеся у предприятий пищевой промышленности и систем водоснабжения на данный момент
	Усилен контроль	Контроль отдельных проб продуктов питания и воды

IV.4. Поскольку условное государство может заметить, что после реализации первых четырех программ темпы снижения риска значительно замедляются, компетентные органы могут в этот момент осуществить оптимальный выбор на диаграмме (отмечен как выбранный вариант). Этот вариант включает в себя следующие усовершенствования: увеличение количества сотрудников полиции в столице, ужесточение процедур в туристическом городе и создание периметра безопасности вокруг места

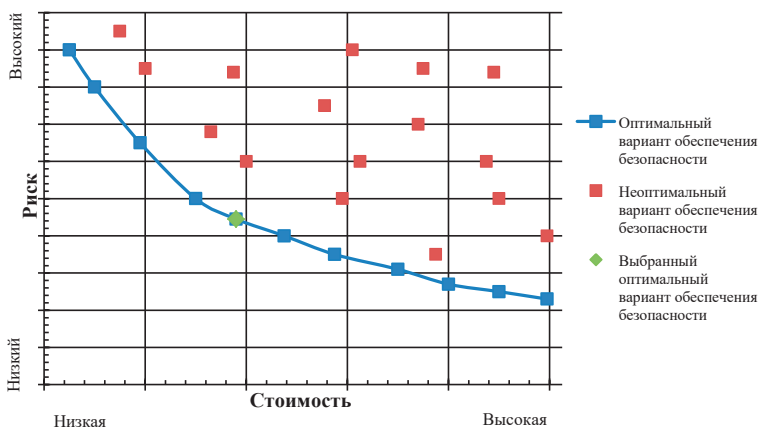


РИС. 11. График анализа затрат-выгод и результатов с указанием вариантов обеспечения безопасности и выбранного варианта.

проведения ежегодного праздника. Следует отметить, что, помимо снижения риска, на это решение могут повлиять и другие факторы. Однако в этом простом примере в число факторов включено только снижение риска.

МЕНЕДЖМЕНТ РИСКОВ

IV.5. При выбранном варианте условное государство внедряет четыре набора систем и мер, используя наилучшую практику управления программами и внедрения систем. В рамках системы менеджмента возможности периметра, используемого при проведении ежегодного национального праздника, отрабатываются на аналогичном, но значительно меньшем по размеру общественном мероприятии, а процессы модифицируются для решения вопросов и проблем, возникающих при проведении такого учения. Модифицированный периметр и процессы применяются в ходе ежегодного праздника. Нанимается и обучается дополнительное количество сотрудников полиции для столичного города. Хотя напрямую измерить потенциальную эффективность этих новых средств в борьбе с потенциальными действиями, имеющими последствия для физической ядерной безопасности, и невозможно (из-за малого количества таких действий), измеряется снижение уровня преступности, которое используется в качестве косвенного показателя улучшенной способности предотвращать действия, имеющие последствия для физической ядерной безопасности. Кроме того, создается макет устройства,

который используется при необъявленных учениях для проверки бдительности правоохранительных органов и оценки их способности обнаруживать и пресекать потенциальное незаконное действие. Наконец, для туристического города разрабатываются новые процедуры, и после их введения оценивается их эффект для туристов и местных жителей.

IV.6. Компетентный орган, ответственный за оценку угроз и рисков, поддерживает информированность о материалах, которые потенциально могут находиться вне регулирующего контроля, путем мониторинга деятельности в условном государстве, а также сведений, поступающих в ITDB, и предупреждений Интерпола. Периодически оценка угроз актуализируется путем включения в нее новой информации о намерениях и возможностях различных злоумышленников. При актуализации оценки угроз актуализируется и оценка рисков. Информация об обновленной оценке рисков доводится до сведения правительства условного государства через компетентный орган на основе принципа служебной необходимости. Параллельно с циклами составления бюджета и проведения закупок выполняется полный процесс менеджмента рисков по мере того, как условное государство раз за разом улучшает свою способность реагировать на действия, имеющие последствия для физической ядерной безопасности, связанные с материалом, находящимся вне регулирующего контроля.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

- [1] Конвенция о физической защите ядерного материала INFCIRC/274/Rev. 1, МАГАТЭ, Вена (1980).
- [2] Международная конвенция о борьбе с актами ядерного терроризма, Резолюция A/RES/59/290, Организация Объединенных Наций, Нью-Йорк (2005).
- [3] МЕЖДУНАРОДНОЕ АГЕНТСТВО ПО АТОМНОЙ ЭНЕРГИИ, Цель и основные элементы государственного режима физической ядерной безопасности, Серия изданий МАГАТЭ по физической ядерной безопасности, № 20, МАГАТЭ, Вена (2014).
- [4] МЕЖДУНАРОДНОЕ АГЕНТСТВО ПО АТОМНОЙ ЭНЕРГИИ, Рекомендации по физической ядерной безопасности, касающиеся физической защиты ядерных материалов и ядерных установок (INFCIRC/225/Revision 5), Серия изданий МАГАТЭ по физической ядерной безопасности, № 13, МАГАТЭ, Вена (2012).
- [5] МЕЖДУНАРОДНОЕ АГЕНТСТВО ПО АТОМНОЙ ЭНЕРГИИ, Рекомендации по физической ядерной безопасности, касающиеся радиоактивных материалов и связанных с ними установок, Серия изданий МАГАТЭ по физической ядерной безопасности, № 14, МАГАТЭ, Вена (2011).
- [6] ВСЕМИРНАЯ ТАМОЖЕННАЯ ОРГАНИЗАЦИЯ, ЕВРОПЕЙСКОЕ ПОЛИЦЕЙСКОЕ УПРАВЛЕНИЕ, МЕЖДУНАРОДНАЯ ОРГАНИЗАЦИЯ ГРАЖДАНСКОЙ АВИАЦИИ, МЕЖДУНАРОДНАЯ ОРГАНИЗАЦИЯ УГОЛОВНОЙ ПОЛИЦИИ — ИНТЕРПОЛ, МЕЖДУНАРОДНОЕ АГЕНТСТВО ПО АТОМНОЙ ЭНЕРГИИ, МЕЖРЕГИОНАЛЬНЫЙ НАУЧНО-ИССЛЕДОВАТЕЛЬСКИЙ ИНСТИТУТ ОРГАНИЗАЦИИ ОБЪЕДИНЕННЫХ НАЦИЙ ПО ВОПРОСАМ ПРЕСТУПНОСТИ И ПРАВОСУДИЯ, УПРАВЛЕНИЕ ОРГАНИЗАЦИИ ОБЪЕДИНЕННЫХ НАЦИЙ ПО НАРКОТИКАМ И ПРЕСТУПНОСТИ, Рекомендации по физической ядерной безопасности, касающиеся ядерных и других радиоактивных материалов, находящихся вне регулирующего контроля, Серия изданий МАГАТЭ по физической ядерной безопасности, № 15, МАГАТЭ, Вена (2011).
- [7] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, Risk Management: Principles and Guidelines, ISO 31000:2009, ISO, Geneva (2009).
- [8] INTERNATIONAL ATOMIC ENERGY AGENCY, Development, Use and Maintenance of the Design Basis Threat, IAEA Nuclear Security Series No. 10, IAEA, Vienna (2009).
- [9] EUROPEAN POLICE OFFICE, INTERNATIONAL ATOMIC ENERGY AGENCY, INTERNATIONAL CRIMINAL POLICE ORGANIZATION, WORLD CUSTOMS ORGANIZATION, Combating Illicit Trafficking in Nuclear and other Radioactive Material, IAEA Nuclear Security Series No. 6, IAEA, Vienna (2007).
- [10] МЕЖДУНАРОДНОЕ АГЕНТСТВО ПО АТОМНОЙ ЭНЕРГИИ, Культура физической ядерной безопасности, Серия изданий МАГАТЭ по физической ядерной безопасности, № 7, МАГАТЭ, Вена (2022).

- [11] МЕЖДУНАРОДНОЕ АГЕНТСТВО ПО АТОМНОЙ ЭНЕРГИИ, Системы и меры физической ядерной безопасности для обнаружения ядерных и других радиоактивных материалов, находящихся вне регулирующего контроля, Серия изданий МАГАТЭ по физической ядерной безопасности, № 21, МАГАТЭ, Вена (2022).
- [12] INTERNATIONAL ATOMIC ENERGY AGENCY, INTERNATIONAL CRIMINAL POLICE ORGANIZATION—INTERPOL, UNITED NATIONS INTERREGIONAL CRIME AND JUSTICE RESEARCH INSTITUTE, Radiological Crime Scene Management, IAEA Nuclear Security Series No. 22-G, IAEA, Vienna (2014).
- [13] СТОЙБЕР К., ШЕРФ А., ТОНХАУЗЕР В., ДЕ ЛУРДЕС ВЕС КАРМОНА М., Справочник по ядерному праву: имплементирующее законодательство, МАГАТЭ, Вена (2010).
- [14] INTERNATIONAL ATOMIC ENERGY AGENCY, IAEA Incident and Trafficking Database (ITDB): Incidents of nuclear and other radioactive material out of regulatory control, 2014 Fact Sheet (2014),
<http://www-ns.iaea.org/downloads/security/itdb-fact-sheet.pdf>.
- [15] International Criminal Police Organization—INTERPOL, Guidelines on Criminal Intelligence Analysis, Version 4 (LEJEUNE, P., MASON-PONTING, J., Eds), Criminal Analysis Sub-Directorate, INTERPOL General Secretariat, Lyon (2002).
- [16] МЕЖДУНАРОДНОЕ АГЕНТСТВО ПО АТОМНОЙ ЭНЕРГИИ, Разработка и применение вероятностной оценки безопасности уровня 1 для атомных электростанций, Серия норм безопасности МАГАТЭ, № SSG-3, МАГАТЭ, Вена (2014).
- [17] Keeney, R.L., von Winterfeldt, d., Eliciting probabilities from experts in complex technical problems, IEEE Trans. Eng. Manage. **38** 3 (1991) 191–201.
- [18] МЕЖДУНАРОДНОЕ АГЕНТСТВО ПО АТОМНОЙ ЭНЕРГИИ, Категоризация радиоактивных источников, Серия норм безопасности МАГАТЭ, № RS-G-1.9, МАГАТЭ, Вена (2006).
- [19] Law, A., Simulation Modeling and Analysis, 4th edn, McGraw-Hill, New York (2006).
- [20] Metropolis, N., Ulam, S., The Monte Carlo Method, J. Am. Stat. Assoc. **44** 247 (1949) 335–341.

ГЛОССАРИЙ

Вне регулирующего контроля. См. регулирующий контроль.

Дифференцированный подход. Применение мер физической ядерной безопасности, соразмерных потенциальным последствиям преступных или преднамеренных несанкционированных действий, совершаемых в отношении ядерного материала, другого радиоактивного материала, соответствующих установок и соответствующей деятельности, или других действий, которые, согласно определению государства, негативно влияют на физическую ядерную безопасность.

Другой радиоактивный материал. Любой радиоактивный материал, который не является ядерным материалом.

Компетентный орган. Государственная организация или учреждение, которому государство поручило выполнение одной или нескольких функций в области физической ядерной безопасности. К компетентным органам могут относиться регулирующие органы, правоохранительные органы, таможенные и пограничные службы, разведывательные службы и органы безопасности, а также учреждения здравоохранения.

Меры физической ядерной безопасности. Меры, имеющие целью предупреждение совершения носителем угрозы физической ядерной безопасности преступных или преднамеренных несанкционированных действий в отношении ядерного материала, другого радиоактивного материала, соответствующих установок или соответствующей деятельности, либо обнаружение событий, связанных с физической ядерной безопасностью, или реагирование на них.

Официальное разрешение. Выдача компетентным органом письменного разрешения на эксплуатацию соответствующей установки или осуществление соответствующей деятельности или документ, дающий такое разрешение.

Оценка риска. Общий процесс систематической идентификации, расчета, анализа и оценивания риска в целях обоснования приоритетных задач, проработки или сопоставления различных направлений действий и подкрепления принимаемых решений.

Оценка угроз. Анализ угроз — на основе имеющейся разведывательной информации, данных правоохранительных органов и информации из открытых источников, — в котором описываются мотивы, намерения и возможности, связанные с этими угрозами.

Оценка уязвимости. Процесс, с помощью которого оцениваются и документируются особенности и эффективность общей системы физической безопасности определенной цели.

Радиационное облучающее устройство (РОУ). Устройство, содержащее радиоактивный материал, которое предназначено для преднамеренного радиационного облучения лиц из населения.

Радиоактивный материал. Любой материал, который в силу своей радиоактивности определен национальным законодательством, регулирующими положениями или регулирующим органом как подлежащий регулирующему контролю. При отсутствии такого определения со стороны государства радиоактивным материалом считается любой материал, защита которого предусмотрена нынешней редакцией Международных основных норм безопасности¹.

Радиологическое диспергирующее устройство (РДУ). Устройство, предназначенное для рассеивания радиоактивного материала при помощи обычных взрывчатых веществ или других средств.

Регулирующий контроль. Любая форма ведомственного контроля, применяемого любым компетентным органом к ядерному материалу или другому радиоактивному материалу, соответствующим установкам или соответствующей деятельности, как того требуют законодательные и регулирующие положения, касающиеся безопасности, физической безопасности или гарантий. Термин «находящийся вне регулирующего контроля» употребляется

¹ АГЕНТСТВО ПО ЯДЕРНОЙ ЭНЕРГИИ ОЭСР, ВСЕМИРНАЯ ОРГАНИЗАЦИЯ ЗДРАВООХРАНЕНИЯ, ЕВРОПЕЙСКАЯ КОМИССИЯ, МЕЖДУНАРОДНАЯ ОРГАНИЗАЦИЯ ТРУДА, МЕЖДУНАРОДНОЕ АГЕНТСТВО ПО АТОМНОЙ ЭНЕРГИИ, ПАНАМЕРИКАНСКАЯ ОРГАНИЗАЦИЯ ЗДРАВООХРАНЕНИЯ, ПРОГРАММА ОРГАНИЗАЦИИ ОБЪЕДИНЕННЫХ НАЦИЙ ПО ОКРУЖАЮЩЕЙ СРЕДЕ, ПРОДОВОЛЬСТВЕННАЯ И СЕЛЬСКОХОЗЯЙСТВЕННАЯ ОРГАНИЗАЦИЯ ОБЪЕДИНЕННЫХ НАЦИЙ, Радиационная защита и безопасность источников излучения: Международные основные нормы безопасности, Серия норм безопасности МАГАТЭ, № GSR Part 3, МАГАТЭ, Вена (2015).

для описания ситуации, когда ядерный материал или другой радиоактивный материал присутствует в достаточном количестве для того, чтобы быть поставленным под регулирующий контроль, но такой контроль отсутствует — в результате утраты контроля по той или иной причине либо вследствие его изначального отсутствия.

Риск. Возможность нежелательного исхода события, связанного с физической ядерной безопасностью, определяемая его вероятностью и соответствующими последствиями.

Самодельное ядерное устройство (СЯУ). Устройство, содержащее радиоактивный материал, которое предназначено для инициирования ядерной реакции с выходом энергии. Такие устройства могут быть полностью самодельными либо представлять собой кустарным способом модифицированное ядерное оружие.

Система физической ядерной безопасности. Комплекс мер физической ядерной безопасности.

Событие, связанное с физической ядерной безопасностью. Событие, имеющее потенциальные или фактические последствия для физической ядерной безопасности, которые требуют принятия соответствующих мер.

Соответствующая деятельность. Обладание ядерным материалом или другим радиоактивным материалом, его производство, переработка, использование, обращение с ним, его хранение, захоронение или перевозка.

Соответствующая установка. Установка (включая связанные с ней здания и оборудование), на которой осуществляется производство, переработка, использование ядерного материала или другого радиоактивного материала, обращение с ним, его хранение или захоронение и для которой требуется официальное разрешение.

Стратегический объект. Особо охраняемый объект в государстве, который является потенциальной целью террористических актов с использованием ядерного материала или другого радиоактивного материала, либо объект, на котором присутствует ядерный или другой радиоактивный материал, находящийся вне регулирующего контроля.

Угроза физической ядерной безопасности. Лицо или группа лиц, имеющие мотивы, намерения и возможности для совершения преступных или преднамеренных несанкционированных действий в отношении ядерного материала, другого радиоактивного материала, соответствующих установок или соответствующей деятельности либо других действий, которые, согласно определению государства, негативно влияют на физическую ядерную безопасность.

Уязвимость. Физическая особенность или эксплуатационное свойство, которое делает учреждение, актив, систему, сеть, установку, деятельность или географический регион открытыми для злоумышленного использования или подверженными определенной угрозе.

Ядерный материал. Любой материал, который представляет собой специальный расщепляющийся материал или исходный материал, как они определены в статье XX Устава МАГАТЭ.



IAEA

Международное агентство по атомной энергии

№ 26

ЗАКАЗ В СТРАНАХ

Платные публикации МАГАТЭ могут быть приобретены у перечисленных ниже поставщиков или в крупных книжных магазинах.

Заказы на бесплатные публикации следует направлять непосредственно в МАГАТЭ. Контактная информация приводится в конце настоящего перечня.

СЕВЕРНАЯ АМЕРИКА

Bernan / Rowman & Littlefield

15250 NBN Way, Blue Ridge Summit, PA 17214, USA

Тел.: +1 800 462 6420 • Факс: +1 800 338 4550

Эл.почта: orders@rowman.com • Сайт: <http://www.rowman.com/bernan>

ОСТАЛЬНЫЕ СТРАНЫ

Просьба связаться с местным поставщиком по вашему выбору или с вашим основным дистрибьютером:

Eurospan Group

Gray's Inn House
127 Clerkenwell Road
London EC1R 5DB
United Kingdom

Торговые заказы и справочная информация:

Тел: +44 (0) 1767604972 • Факс: +44 (0) 1767601640

Эл.почта: eurospan@turpin-distribution.com

Индивидуальные заказы:

www.eurospanbookstore.com/iaea

Дополнительная информация:

Тел: +44 (0) 2072400856 • Факс: +44 (0) 2073790609

Эл.почта: info@eurospangroup.com • Сайт: www.eurospangroup.com

Заказы на платные и бесплатные публикации можно направлять напрямую по адресу:

Группа маркетинга и сбыта (Marketing and Sales Unit)

Международное агентство по атомной энергии

Vienna International Centre, PO Box 100, 1400 Vienna, Austria

Телефон: +43 1 2600 22529 или 22530 • Факс: +43 1 26007 22529

Эл.почта: sales.publications@iaea.org • Сайт: <https://www.iaea.org/ru/publikacii>

Угроза ядерного терроризма вызывает обеспокоенность у всех государств, а риск использования ядерного или другого радиоактивного материала в преступных целях несет в себе серьезную угрозу национальной и международной безопасности с потенциально серьезными последствиями для людей, имущества и окружающей среды. В данном практическом руководстве описываются концепции и методики применения риск-ориентированного подхода при планировании, разработке и внедрении мер физической ядерной безопасности ядерного и другого радиоактивного материала, находящегося вне регулирующего контроля.