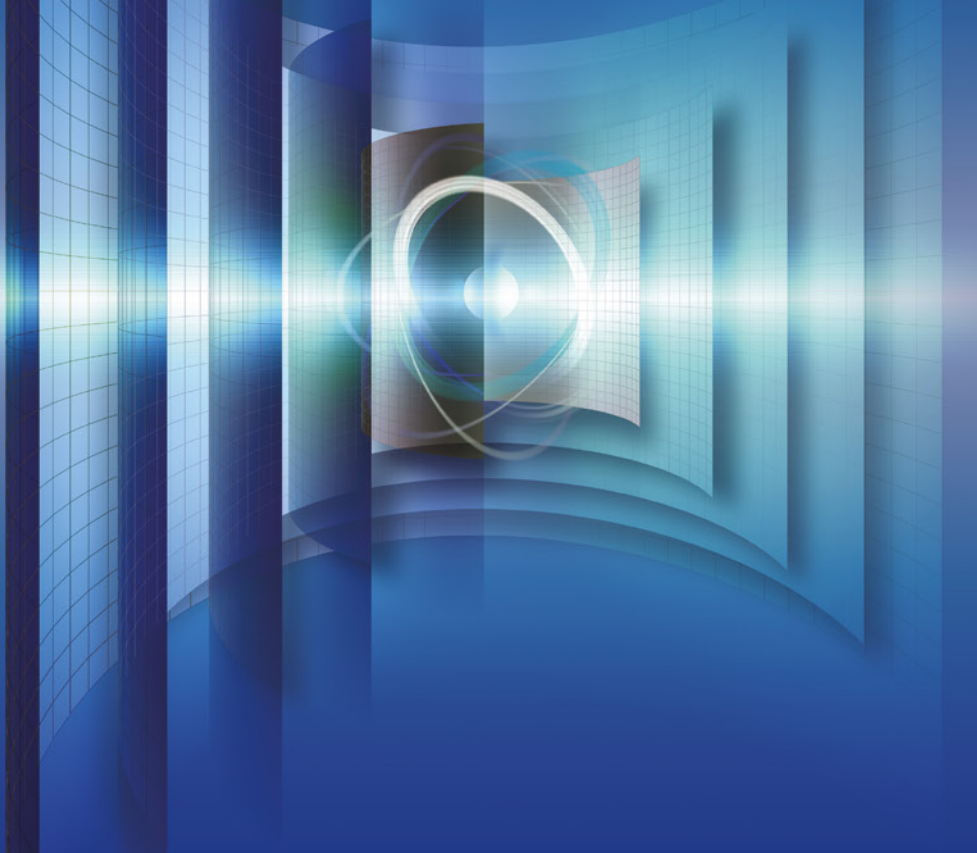
Серия изданий МАГАТЭ по физической ядерной безопасности, № 10-G (Rev. 1)

Практическое руководство

Оценка угроз физической ядерной безопасности на национальном уровне, проектные угрозы и профили характерных угроз



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.

ОЦЕНКА УГРОЗ ФИЗИЧЕСКОЙ ЯДЕРНОЙ БЕЗОПАСНОСТИ НА НАЦИОНАЛЬНОМ УРОВНЕ, ПРОЕКТНЫЕ УГРОЗЫ И ПРОФИЛИ ХАРАКТЕРНЫХ УГРОЗ

Членами Международного агентства по атомной энергии являются следующие государства:

АВСТРАЛИЯ
АВСТРИЯ
АЗЕРБАЙДЖАН
АЛБАНИЯ
АЛЖИР
АНГОЛА
АНТИГУА И БАРБУДА
АРГЕНТИНА
АРМЕНИЯ
АФГАНИСТАН
БАГАМСКИЕ ОСТРОВА
БАНГЛАДЕШ
БАРБАДОС
БАХРЕЙН
БЕЛАРУСЬ
БЕЛИЗ
БЕЛЬГИЯ
БЕНИН
БОЛГАРИЯ
БОЛИВИЯ, МНОГОНАЦИОНАЛЬНОЕ ГОСУДАРСТВО
БОСНИЯ И ГЕРЦЕГОВИНА
БОТСВАНА
БРАЗИЛИЯ
БРУНЕЙ-ДАРУССАЛАМ
БУРКИНА-ФАСО
БУРУНДИ
ВАНУАТУ
ВЕНГРИЯ
ВЕНЕСУЭЛА, БОЛИВАРИАНСКАЯ РЕСПУБЛИКА
ВЬЕТНАМ
ГАБОН
ГАИТИ
ГАЙАНА
ГАМБИЯ
ГАНА
ГВАТЕМАЛА
ГВИНЕЯ
ГЕРМАНИЯ
ГОНДУРАС
ГРЕНАДА
ГРЕЦИЯ
ГРУЗИЯ
ДАНИЯ
ДЕМОКРАТИЧЕСКАЯ РЕСПУБЛИКА КОНГО
ДЖИБУТИ
ДОМИНИКА
ДОМИНИКАНСКАЯ РЕСПУБЛИКА
ЕГИПЕТ
ЗАМБИЯ
ЗИМБАБВЕ
ИЗРАИЛЬ
ИНДИЯ
ИНДОНЕЗИЯ
ИОРДАНИЯ
ИРАК
ИРАН, ИСЛАМСКАЯ РЕСПУБЛИКА
ИРЛАНДИЯ
ИСЛАНДИЯ
ИСПАНИЯ
ИТАЛИЯ
ЙЕМЕН
КАБО-ВЕРДЕ
КАЗАХСТАН
КАМБОДЖА
КАМЕРУН
КАНАДА
КАТАР
КЕНИЯ
КИПР
КИТАЙ
КОЛУМБИЯ
КОМОРСКИЕ ОСТРОВА
КОНГО
КОРЕЯ, РЕСПУБЛИКА
КОСТА-РИКА
КОТ-Д'ИВУАР
КУБА
КУВЕЙТ
КЫРГЫЗСТАН
ЛАОССКАЯ НАРОДНО-ДЕМОКРАТИЧЕСКАЯ РЕСПУБЛИКА
ЛАТВИЯ
ЛЕСОТО
ЛИБЕРИЯ
ЛИВАН
ЛИВИЯ
ЛИТВА
ЛИХТЕНШТЕЙН
ЛЮКСЕМБУРГ
МАВРИКИЙ
МАВРИТАНИЯ
МАДАГАСКАР
МАЛАВИ
МАЛАЙЗИЯ
МАЛИ
МАЛЬТА
МАРОККО
МАРШАЛЛОВЫ ОСТРОВА
МЕКСИКА
МОЗАМБИК
МОНАКО
МОНГОЛИЯ
МЬЯНМА
НАМИБИЯ
НЕПАЛ
НИГЕР
НИГЕРИЯ
НИДЕРЛАНДОВ, КОРОЛЕВСТВО
НИКАРАГУА
НОВАЯ ЗЕЛАНДИЯ
НОРВЕГИЯ
ОБЪЕДИНЕННАЯ РЕСПУБЛИКА ТАНЗАНИЯ
ОБЪЕДИНЕННЫЕ АРАБСКИЕ ЭМИРАТЫ
ОМАН
ПАКИСТАН
ПАЛАУ
ПАНАМА
ПАПУА — НОВАЯ ГВИНЕЯ
ПАРАГВАЙ
ПЕРУ
ПОЛЬША
ПОРТУГАЛИЯ
РЕСПУБЛИКА МОЛДОВА
РОССИЙСКАЯ ФЕДЕРАЦИЯ
РУАНДА
РУМЫНИЯ
САЛЬВАДОР
САМОА
САН-МАРИНО
САУДОВСКАЯ АРАВИЯ
СВЯТОЙ ПРЕСТОЛ
СЕВЕРНАЯ МАКЕДОНИЯ
СЕЙШЕЛЬСКИЕ ОСТРОВА
СЕНЕГАЛ
СЕНТ-ВИНСЕНТ И ГРЕНАДИНЫ
СЕНТ-КИТС И НЕВИС
СЕНТ-ЛЮСИЯ
СЕРБИЯ
СИНГАПУР
СИРИЙСКАЯ АРАБСКАЯ РЕСПУБЛИКА
СЛОВАКИЯ
СЛОВЕНИЯ
СОЕДИНЕННОЕ КОРОЛЕВСТВО ВЕЛИКОБРИТАНИИ И СЕВЕРНОЙ ИРЛАНДИИ
СОЕДИНЕННЫЕ ШТАТЫ АМЕРИКИ
СУДАН
СЬЕРРА-ЛЕОНЕ
ТАДЖИКИСТАН
ТАИЛАНД
ТОГО
ТОНГА
ТРИНИДАД И ТОБАГО
ТУНИС
ТУРКМЕНИСТАН
ТУРЦИЯ
УГАНДА
УЗБЕКИСТАН
УКРАИНА
УРУГВАЙ
ФИДЖИ
ФИЛИППИНЫ
ФИНЛЯНДИЯ
ФРАНЦИЯ
ХОРВАТИЯ
ЦЕНТРАЛЬНОАФРИКАНСКАЯ РЕСПУБЛИКА
ЧАД
ЧЕРНОГОРИЯ
ЧЕШСКАЯ РЕСПУБЛИКА
ЧИЛИ
ШВЕЙЦАРИЯ
ШВЕЦИЯ
ШРИ-ЛАНКА
ЭКВАДОР
ЭРИТРЕЯ
ЭСВАТИНИ
ЭСТОНИЯ
ЭФИОПИЯ
ЮЖНАЯ АФРИКА
ЯМАЙКА
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, № 10-G (Rev. 1)

ОЦЕНКА УГРОЗ ФИЗИЧЕСКОЙ ЯДЕРНОЙ БЕЗОПАСНОСТИ НА НАЦИОНАЛЬНОМ УРОВНЕ, ПРОЕКТНЫЕ УГРОЗЫ И ПРОФИЛИ ХАРАКТЕРНЫХ УГРОЗ

ПРАКТИЧЕСКОЕ РУКОВОДСТВО

МЕЖДУНАРОДНОЕ АГЕНТСТВО ПО АТОМНОЙ ЭНЕРГИИ
ВЕНА, 2024

УВЕДОМЛЕНИЕ ОБ АВТОРСКОМ ПРАВЕ

Издательская секция (Publishing Section)
Международное агентство по атомной энергии
Венский международный центр,
а/я 100,
A1400 Вена, Австрия
тел.: +43 1 2600 22529 или 22530
эл. почта: sales.publications@iaea.org
https://www.iaea.org/ru/publikacii

Отпечатано МАГАТЭ в Австрии
Ноябрь, 2024
STI/PUB/1926

ОЦЕНКА УГРОЗ ФИЗИЧЕСКОЙ ЯДЕРНОЙ БЕЗОПАСНОСТИ НА НАЦИОНАЛЬНОМ УРОВНЕ, ПРОЕКТНЫЕ УГРОЗЫ И ПРОФИЛИ ХАРАКТЕРНЫХ УГРОЗ
МАГАТЭ, ВЕНА, 2024 ГОД
STI/PUB/1926
ISBN 978-92-0-407824-4 (печатный формат) ISBN 978-92-0-407624-0 (формат pdf) ISBN 978-92-0-407724-7 (формат epub)
ISSN 2788-8959

ПРЕДИСЛОВИЕ

Рафаэль Мариано Гросси
Генеральный директор

В Серию изданий МАГАТЭ по физической ядерной безопасности входят согласованные на основе международного консенсуса руководящие материалы по всем аспектам физической ядерной безопасности, призванные поддерживать государства в их работе по выполнению своих обязанностей в области физической ядерной безопасности. В рамках своей центральной роли по обеспечению международной поддержки и координации в области физической ядерной безопасности, МАГАТЭ разрабатывает и утверждает эти руководящие материалы и поддерживает их актуальность.

Публикации Серии изданий МАГАТЭ по физической ядерной безопасности впервые увидели свет в 2006 году и с тех пор постоянно обновляются МАГАТЭ в сотрудничестве с экспертами из государств-членов. Как Генеральный директор я разделяю стремление к тому, чтобы МАГАТЭ и далее поддерживало и совершенствовало эту всеобъемлющую, многогранную и последовательную серию изданий, в которой выходят актуальные, удобные для пользователя и соответствующие поставленным целям руководящие материалы по вопросам физической безопасности, неизменно высокого качества. Надлежащее применение этих руководящих материалов при использовании ядерной науки и технологий позволит достичь высокого уровня физической ядерной безопасности и обеспечить необходимую уверенность для непрерывного использования ядерных технологий ради всеобщего блага.

Обеспечение физической ядерной безопасности относится к сфере ответственности государства. Серия изданий МАГАТЭ по физической ядерной безопасности дополняет международно-правовые документы по физической ядерной безопасности и служит глобальным источником информации, которым могут руководствоваться стороны при выполнении своих обязательств. Хотя эти руководящие материалы по физической ядерной безопасности не имеют для государств-членов обязательной юридической силы, они широко применяются на практике. Они выполняют функцию незаменимого источника информации и общего знаменателя для подавляющего большинства государств-членов, которые внедрили эти руководящие принципы в свои национальные регулирующие положения в целях укрепления физической ядерной безопасности на ядерных энергетических установках, исследовательских реакторах и установках

топливного цикла, а также в области применения ядерных технологий в медицине, промышленности, сельском хозяйстве и научных исследованиях.

Руководящие материалы, представленные в Серии изданий МАГАТЭ по физической ядерной безопасности, обобщают практический опыт государств-членов и подготовлены на основе международного консенсуса. Особенно важное значение имеет то, что в их разработке принимают участие члены Комитета по руководящим материалам по физической ядерной безопасности и другие эксперты, и я признателен всем тем, кто привносит в эту деятельность свои знания и опыт.

Со своей стороны МАГАТЭ также опирается на публикуемые в Серии изданий МАГАТЭ по физической ядерной безопасности руководящие материалы, когда оказывает помощь государствам-членам в рамках своих миссий по экспертной оценке и консультационных услуг. Это облегчает государствам-членам применение данных рекомендаций на практике и создает условия для обмена ценным опытом и аналитическими наработками. Руководящие материалы по физической ядерной безопасности периодически пересматриваются с учетом отзывов, полученных по итогам соответствующих миссий и услуг, уроков, извлеченных в результате тех или иных событий, а также опыта работы с такими материалами.

Я убежден, что руководящие материалы, представленные в Серии изданий МАГАТЭ по физической ядерной безопасности, как и практика их применения, вносят неоценимый вклад в обеспечение высокого уровня физической ядерной безопасности во всех сферах, где используются ядерные технологии. Я призываю все государства-члены способствовать более широкому применению этих руководящих материалов и сотрудничать с МАГАТЭ в интересах поддержания их качества как в реалиях сегодняшнего дня, так и в будущем.

РЕДАКЦИОННОЕ ПРИМЕЧАНИЕ

Руководящие материалы, изданные в Серии изданий МАГАТЭ по физической ядерной безопасности, не являются обязательными для государств, однако государства могут использовать эти руководящие материалы в качестве подспорья для выполнения ими своих обязательств по международно-правовым документам, а также для осуществления ими своих обязанностей 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 фигурируют, или в руководящих материалах более высокого уровня, на которые опирается эта публикация. Во всех остальных случаях слова употребляются в их общепринятых значениях.

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

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

Использование тех или иных названий стран или территорий не означает какого-либо суждения со стороны издателя — МАГАТЭ — относительно правового статуса таких стран или территорий, их органов и учреждений либо относительно определения их границ.

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

СОДЕРЖАНИЕ

1. ВВЕДЕНИЕ

ОБЩИЕ СВЕДЕНИЯ

1.1. Публикации категории «Основы физической ядерной безопасности» определяют цель национального режима физической ядерной безопасности и его основные элементы [1]. Публикации категории «Рекомендации по физической ядерной безопасности» указывают на вопросы, которые рассматриваются в рамках режима физической ядерной безопасности в связи со следующим материалом и связанными с ним установками:

a) ядерным материалом и ядерными установками [2];
b) радиоактивным материалом и связанными с ним установками [3];
c) ядерным и другим радиоактивным материалом, находящимся вне регулирующего контроля [4].

1.2. Заложить необходимую основу для выбора, разработки и реализации мер физической ядерной безопасности позволяет идентификация и оценка соответствующих угроз. В контексте ядерного материала и другого радиоактивного материала, находящегося под регулирующим контролем, а также связанных с ним установок и видов деятельности результатом такой идентификации и оценки является определение так называемой проектной угрозы или профилей характерных угроз, отражающих намерения и возможности потенциальных злоумышленников, от действий которых должны быть защищены материалы и связанные с ним установки и виды деятельности.

1.3. Настоящая публикация представляет собой пересмотренный вариант документа Серии изданий МАГАТЭ по физической ядерной безопасности, № 10, «Development, Use and Maintenance of the Design Basis Threat»[1] («Разработка, использование и актуализация критериев проектной угрозы»), который ставит своей целью обобщить происшедшие в этой области изменения и обеспечить согласованность терминологии с документами [1–4], опубликованными после 2009 года.

---

[1] INTERNATIONAL ATOMIC ENERGY AGENCY, Development, Use and Maintenance of the Design Basis Threat, IAEA Nuclear Security Series No. 10, IAEA, Vienna (2009).

1.4. Кроме того, сфера применения данной публикации была расширена с целью уточнить порядок применения альтернативного подхода к определению проектной угрозы, разъяснить аспекты проработки проектной угрозы для отдельных сфер применения и уделить более пристальное внимание угрозам, связанным с кибератаками [5].

ЦЕЛЬ

1.5. Цель настоящей публикации — представить поэтапную методологию проведения оценки угроз физической ядерной безопасности на национальном уровне, включающую в себя аспекты физической и компьютерной безопасности, а также порядок разработки, применения и актуализации проектной угрозы и профилей характерных угроз. Речь идет о следующих этапах:

a) определение функций и обязанностей государства, компетентных органов (включая регулирующий орган[2]) и операторов;
b) идентификация и оценка угроз, связанных с физической ядерной безопасностью;
c) разработка моделей угроз, таких как проектная угроза и профили характерных угроз, с использованием результатов, которые были получены при проведении оценки угроз физической ядерной безопасности на национальном уровне;
d) использование проектной угрозы и/или профилей характерных угроз для разработки систем и мер физической ядерной безопасности, а также требований к физической ядерной безопасности;
e) поддержание в актуальном состоянии оценки угроз физической ядерной безопасности на национальном уровне и ее документирования;
f) поддержание в актуальном состоянии данных, касающихся проектной угрозы и профилей характерных угроз.

1.6. Настоящая публикация предназначена для использования государствами, компетентными органами (включая регулирующий орган), соответствующими организациями научно-технической поддержки,

[2] В некоторых государствах вопросы физической ядерной безопасности ядерного материала и другого радиоактивного материала, а также связанных с ним установок и видов деятельности относятся к сфере ведения нескольких регулирующих органов. В настоящей публикации термин «регулирующий орган» означает орган (или органы), сообразный данному контексту.

а также операторами установок и видов деятельности, связанных с ядерным материалом и другим радиоактивным материалом, включая грузоотправителей и перевозчиков.

СФЕРА ПРИМЕНЕНИЯ

1.7. Представленные в этой публикации концепция и методология применяются при проведении оценки угроз физической ядерной безопасности на национальном уровне, включая аспекты физической и компьютерной безопасности, а также при разработке, применении и актуализации проектной угрозы и профилей характерных угроз в целях защиты ядерного и другого радиоактивного материала, находящегося под регулирующим контролем, и связанных с ним установок и видов деятельности.

1.8. За рамками настоящей публикации находятся руководящие указания по разработке риск-ориентированного подхода и по проведению оценки угроз и рисков, которые могут быть положены в основу обеспечения физической ядерной безопасности ядерного и другого радиоактивного материала, находящегося вне регулирующего контроля. Рекомендации по данному вопросу представлены в публикации Серии изданий МАГАТЭ по физической ядерной безопасности, № 24-G, «Риск-ориентированный подход к мерам физической ядерной безопасности в отношении ядерного и другого радиоактивного материала, находящегося вне регулирующего контроля» [6].

СТРУКТУРА

1.9. Раздел 2, следующий за вводной частью, посвящен оценке угроз физической ядерной безопасности на национальном уровне в рамках применения риск-ориентированного подхода. В разделе 3 представлены общие сведения о процессе оценки угроз физической ядерной безопасности на национальном уровне и подготовке, использовании и поддержании в актуальном состоянии оценки угроз и соответствующей документации, а также проектных угроз и профилей характерных угроз. В разделе 4 определены функции и обязанности организаций, участвующих в процессе оценки угроз физической ядерной безопасности на национальном уровне. В разделе 5 содержатся более подробные рекомендации по проведению оценки угроз физической ядерной безопасности на национальном уровне. В разделе 6 рассказывается о разработке моделей проектной угрозы и

профилей характерных угроз, а в разделе 7 даны рекомендации по их использованию. Раздел 8 содержит рекомендации по поддержанию в актуальном состоянии оценки угроз физической ядерной безопасности на национальном уровне и соответствующей документации, а также профилей характерных угроз. В дополнении к настоящей публикации приводится пример описания проектной угрозы.

2. ОЦЕНКА УГРОЗ ФИЗИЧЕСКОЙ ЯДЕРНОЙ БЕЗОПАСНОСТИ НА НАЦИОНАЛЬНОМ УРОВНЕ И ИСПОЛЬЗОВАНИЕ РИСК-ОРИЕНТИРОВАННОГО ПОДХОДА

2.1. Международные конвенции и руководящие материалы Серии изданий МАГАТЭ по физической ядерной безопасности указывают на важность оценки угроз физической ядерной безопасности и применения в этом контексте риск-ориентированного подхода. Примечательно, что основополагающий принцип G (Угроза) Конвенции о физической защите ядерного материала с поправками [7, 8], а также документ [2] указывают на следующее: **«государственную систему физической защиты следует основывать на проводимой государством текущей оценке угрозы»**.

2.2. Основной элемент 9, представленный в документе [1], заключается в следующем:

> «В *режиме физической ядерной безопасности* применяются подходы, учитывающие факторы риска, в том числе при выделении ресурсов на *системы физической ядерной безопасности* и *меры по обеспечению физической ядерной безопасности* и при проведении мероприятий, связанных с физической ядерной безопасностью, которые базируются на *дифференцированном подходе* и *глубокоэшелонированной защите*, в которых учитывается следующее:
>
> a) текущая оценка государством *угроз физической ядерной безопасности* как внутренних, так и внешних;
> b) относительная привлекательность выявленных *целей* для носителей *угрозы физической ядерной безопасности* и их уязвимость перед такими угрозами;

c) характеристики *ядерного материала*, *другого радиоактивного материала*, *соответствующих установок* и *соответствующей деятельности*;

d) потенциальные вредные последствия преступных или преднамеренных несанкционированных действий в отношении *ядерного материала*, *другого радиоактивного материала*, *соответствующих установок*, *соответствующей деятельности*, *чувствительной информации или активов чувствительной информации* и других действий, которые, согласно определению государства, могут негативно повлиять на физическую ядерную безопасность».

2.3. Кроме того, в пункте 3.10 документа [2] сказано:

«Государству следует определять на основе *оценки угроз* или *проектной угрозы* требования к физической защите *ядерных материалов* при их использовании и хранении и при *перевозке* (транспортировке), а также *ядерных установок* в зависимости от соответствующих последствий, связанных с любым *несанкционированным изъятием* или *саботажем (диверсией)*».

Пункты 3.17 и 3.18 документа [3] гласят:

«Государству следует проводить оценку национальных *угроз* применительно к *радиоактивным материалам, связанным с ними установкам* и *связанной с ними деятельности*. Государству следует периодически рассматривать национальные *угрозы* и оценивать последствия любых изменений этих *угроз* для формирования или модернизации своего *режима физической ядерной безопасности*». «*Регулирующему органу* следует использовать результаты *оценки угроз* в качестве общей основы для определения требований по обеспечению физической безопасности, действующих в отношении *радиоактивных материалов*, и для периодической оценки их адекватности».

2.4. В нижеследующих подразделах более подробно рассматриваются некоторые вопросы, касающиеся оценки угроз физической ядерной безопасности на национальном уровне с использованием риск-ориентированного подхода; касающиеся злоумышленников, их признаков и характеристик; а также касающиеся информационной безопасности.

РИСК-ОРИЕНТИРОВАННЫЙ ПОДХОД И ПРОФИЛИ УГРОЗ

2.5. Основной элемент 9 режима физической ядерной безопасности [1] предполагает применение риск-ориентированных подходов, в том числе при выделении ресурсов на системы физической ядерной безопасности и меры по обеспечению физической ядерной безопасности и при проведении мероприятий, связанных с физической ядерной безопасностью, которые базируются на дифференцированном подходе и глубокоэшелонированной защите. При применении риск-ориентированного подхода к физической ядерной безопасности следует принимать во внимание такие аспекты, как угроза, привлекательность и уязвимость потенциальных целей и потенциальные последствия, которые могут возникнуть в результате злоумышленных действий.

2.6. Пункт 3.41 документа [2] содержит следующую рекомендацию: «Государству следует посредством управления риском обеспечивать способность государственного *режима физической защиты* ограничивать и удерживать риски *несанкционированного изъятия* и *саботажа (диверсии)* на приемлемом уровне». Необходимо, чтобы процесс управления рисками включал в себя периодическую переоценку угроз и потенциальных последствий злоумышленных действий и обеспечивал наличие надлежащих систем и мер физической ядерной безопасности для предотвращения или снижения вероятности успешного совершения злоумышленного действия.

2.7. Оценка угроз физической ядерной безопасности на национальном уровне — это анализ существующих угроз, связанных с физической ядерной безопасностью, который включает в себя аспекты физической и компьютерной безопасности и проводится с целью определить признаки и характеристики потенциальных злоумышленников. В этом процессе оценки угроз физической ядерной безопасности на национальном уровне используются глобальные, региональные и национальные источники информации.

2.8. Результаты процесса оценки угроз физической ядерной безопасности на национальном уровне заносятся в документацию по оценке угроз физической ядерной безопасности на национальном уровне и могут быть использованы для разработки профилей угроз. Профиль угрозы содержит правдоподобные признаки и характеристики потенциальных злоумышленников, от действий которых должны быть защищены деятельность и установки, связанные с ядерным материалом и другим радиоактивным материалом.

2.9. Содержащаяся в таких моделях угроз, как проектная угроза и профили характерных угроз, оценка существующих угроз, связанных с физической ядерной безопасностью, может быть использована с целью облегчить применение риск-ориентированного подхода к физической ядерной безопасности и управление рисками в отношении отдельных установок и видов деятельности. Профили угроз могут быть полезны при разработке и оценке систем и мер обеспечения физической ядерной безопасности, в которых учитываются потенциальные последствия успешного злоумышленного действия.

2.10. Государства могут по своему усмотрению прорабатывать эти модели либо в виде проектных угроз, либо в виде профилей характерных угроз или же использовать и то и другое наряду с надлежащим подходом к нормативному регулированию[3] различных типов установок и видов деятельности. Профиль характерных угроз может использоваться для разработки нормативных требований, преимущественно содержащих предписывающие требования к определенному набору подлежащих защите материалов или установок, воздействие на которые влечет за собой менее значительные последствия; в то время как проектная угроза может быть сформулирована для случаев применения нормативных требований, где предпочтение отдается подходу, ориентированному на достижение определенных показателей, для защиты отдельных установок или деятельности, воздействие на которые влечет за собой более значительные последствия. Так, профиль характерных угроз может использоваться компетентным органом для разработки предписывающих нормативных требований по защите радиоактивных источников категории 1 в процессе их использования и хранения, в то время как проектная угроза может использоваться оператором для разработки и оценки системы физической ядерной безопасности с целью соответствия требованиям, ориентированным на достижение определенных показателей, для обеспечения эффективной защиты конкретного радиоактивного источника категории 1 при различных сценариях воздействия.

2.11. На основании результатов проведенной на национальном уровне оценки угроз физической ядерной безопасности государства могут по своему усмотрению определять различные профили характерных угроз исходя из различных категорий ядерного материала и другого радиоактивного

---

[3] Более подробная информация о предписывающем подходе к нормативному регулированию и подходе, ориентированном на достижение определенных показателей, содержится в [2, 3, 8, 9].

материала, различных типов установок и видов деятельности (например, радиоактивные источники категории 1, облучатели и перевозка радиоактивного материала), различных целей злоумышленников (например, хищение и саботаж) и активов, которые могут выбираться в качестве объекта целенаправленных кибератак (например, конфиденциальная информация или компьютеризированные системы, используемые для обеспечения ядерной и физической безопасности, учета и контроля ядерного материала, а также при аварийном реагировании).

2.12. Аналогичным образом, на основании результатов проведенной на национальном уровне оценки угроз физической ядерной безопасности государства могут по своему усмотрению определять различные проектные угрозы, применимые к материалам, которые используются на конкретных установках или в рамках деятельности, сопряженной с повышенными рисками (например, исследовательские реакторы и перевозка отработавшего ядерного топлива). В этих моделях проектной угрозы учитываются особенности конкретных установок или видов деятельности (например, конструкция и расположение), принципиальные соображения (например, необходимая для поддержания доверия населения степень консерватизма), а также возможности и ресурсы государства и оператора.

2.13. Некоторые угрозы, выявленные в процессе оценки угроз физической ядерной безопасности на национальном уровне, будут, вероятно, исключены из проектной угрозы или профилей характерных угроз, поскольку они могут быть сочтены выходящими за рамки проектных основ. Даже при условии обеспечения системой физической ядерной безопасности оператора некоторых внутренне присущих функций защиты необходимо, чтобы защита от этих угроз предусматривалась также и в плане чрезвычайных мер государства благодаря координации мер реагирования государства и плана чрезвычайных мер реагирования оператора. И хотя именно государству следует разрабатывать меры по противодействию этим угрозам, оператору может все же быть отведена определенная роль в оказании государству помощи в части защиты от этих угроз физической ядерной безопасности или смягчения их последствий.

2.14. Решения, касающиеся рисков физической ядерной безопасности, принимаются исходя из текущих угроз, которые вызывают опасения у государства, вероятности возникновения новых угроз, а также решений о том, как уравновешиваются между собой соображения консерватизма, затраты и эксплуатационные последствия. Кроме того, такие решения могут учитывать международные и региональные угрозы, политические и финансовые

факторы, восприятие риска населением, а также уроки, извлеченные по итогам оценок угроз физической ядерной безопасности в прошлом.

ПОТЕНЦИАЛЬНЫЕ ЗЛОУМЫШЛЕННИКИ, ИХ ПРИЗНАКИ И ХАРАКТЕРИСТИКИ

2.15. К потенциальным злоумышленникам можно отнести террористов, прочих преступников и экстремистов, которые могут стремиться приобрести и использовать ядерный или другой радиоактивный материал для создания ядерных взрывных устройств, радиологических диспергирующих устройств или устройств радиационного воздействия. Такие злоумышленники могут пытаться также организовать акты саботажа (диверсии), целью которых являются установки, где используется или хранится ядерный или другой радиоактивный материал, или перевозка такого материала.

2.16. Потенциального злоумышленника отличает наличие мотивации, умысла и возможностей. Например, мотивация может быть финансовой, политической или идеологической либо стать следствием недовольства или принуждения. Умысел может быть направлен на несанкционированное завладение ядерным материалом или другим радиоактивным материалом, получение конфиденциальной информации или конфиденциальных информационных активов, нанесение ущерба путем саботажа (диверсии) или формирование негативного общественного резонанса вокруг оператора установки или соответствующего вида деятельности, либо государства. Возможности злоумышленника зависят от таких характеристик, как число вовлеченных в злоумышленные действия лиц, уровень их организации и координации, а также наличие инсайдеров. К возможностям относятся также способности, активы и соответствующие навыки отдельных людей и организаций, такие как тактика, вооружение, взрывчатые вещества, транспорт, физические и компьютерные инструменты, знание уязвимостей программного обеспечения и уровень доступа к установке или ее компьютеризированным системам.

2.17. Злоумышленником может оказаться инсайдер [9]: лицо, имеющее официальный доступ к соответствующим установкам или видам деятельности либо к конфиденциальной информации или конфиденциальным информационным активам, которое может совершать или содействовать совершению преступных или преднамеренных несанкционированных действий, связанных с ядерным материалом, другим радиоактивным материалом, соответствующими установками или видами

деятельности либо направленных на них, равно как и других действий, которые, согласно определению государства, могут негативно повлиять на физическую ядерную безопасность. Злоумышленники могут стремиться стать инсайдерами, получив официальный доступ к установке (например, работая по найму в качестве штатного сотрудника либо подрядчика), чтобы в дальнейшем воспользоваться этим доступом; или же инсайдерскую угрозу могут представлять собой уже нанятые сотрудники, у которых возникает либо формируется извне намерение совершить злоумышленные действия или потворствовать им.

2.18. Необходимо учитывать также возможность сговора между инсайдерами и внешними злоумышленниками. Например, инсайдер может физически либо с помощью компьютеризированных средств совершить несанкционированное действие с целью содействовать совершению злоумышленного действия внешним злоумышленником.

2.19. Государствам следует принимать во внимание не только потенциальные злоумышленные действия, связанные с физическим доступом к установке или деятельности, но и совершаемые посредством кибератак. Целью таких атак могут быть компьютерные системы, которые используются для обеспечения ядерной безопасности (включая системы контроля и управления), учета и контроля ядерного материала, обеспечения физической ядерной безопасности или аварийного реагирования (включая системы связи и сигнализации). Злоумышленники могут предпринимать также попытки «смешанного» нападения, когда атака на компьютерную систему проводится в сочетании с физическим нападением, как, например, вооруженное вторжение с использованием поддельных электронных реквизитов доступа в целях саботажа (диверсии) или хищения материала.

2.20. Необходимо учитывать возможность совершения как инсайдерами, так и внешними злоумышленниками действий, в результате которых под угрозу будет поставлена конфиденциальность, целостность и доступность информации в компьютерных системах. Такие действия могут осуществлять как инсайдеры, так и внешние злоумышленники посредством удаленной кибератаки. Необходимо учитывать также возможность внедрения в компьютерные системы вредоносных программ в рамках цепочки поставок.

2.21. Необходимо учитывать также возможность нанесения ударов извне. При нанесении таких ударов могут использоваться устройства, управление которыми происходит на расстоянии, такие как БПЛА, ракетное оружие или оружие направленной энергии.

2.22. При разработке и поддержании в актуальном состоянии профилей угроз необходимо учитывать всю достоверную информацию, имеющую отношение к угрозам, включая данные национальной разведки и другую конфиденциальную информацию. Необходимо обеспечить защиту определенной части этой информации и многих ее источников. Используемые при разработке и оценке систем физической ядерной безопасности модели проектной угрозы или профили характерных угроз подлежат защите в качестве конфиденциальной информации — то есть информации в любой форме, включая программное обеспечение, несанкционированное раскрытие, корректировка, изменение, уничтожение или неиспользование которой может поставить физическую ядерную безопасность под угрозу.

2.23. Подробные рекомендации по защите конфиденциальной информации, касающейся физической ядерной безопасности, содержатся в публикации Серии изданий МАГАТЭ по физической ядерной безопасности, № 23-G, «Безопасность ядерной информации» [10].

3. ОБЩИЕ СВЕДЕНИЯ О ПРОЦЕССЕ РАЗРАБОТКИ, ИСПОЛЬЗОВАНИЯ И ПОДДЕРЖАНИЯ В АКТУАЛЬНОМ СОСТОЯНИИ ОЦЕНКИ УГРОЗ ФИЗИЧЕСКОЙ ЯДЕРНОЙ БЕЗОПАСНОСТИ НА НАЦИОНАЛЬНОМ УРОВНЕ И СООТВЕТСТВУЮЩЕЙ ДОКУМЕНТАЦИИ, ПРОЕКТНЫХ УГРОЗ И ПРОФИЛЕЙ ХАРАКТЕРНЫХ УГРОЗ

3.1. На рис. 1 представлен процесс разработки, использования и поддержания в актуальном состоянии оценки угроз физической ядерной безопасности на национальном уровне и соответствующей документации, а также проектных угроз и профилей характерных угроз. Этот процесс состоит из пяти этапов:

1) определение функций и обязанностей;
2) проведение и документирование оценки угроз физической ядерной безопасности на национальном уровне;
3) разработка моделей проектной угрозы и/или профилей характерных угроз;

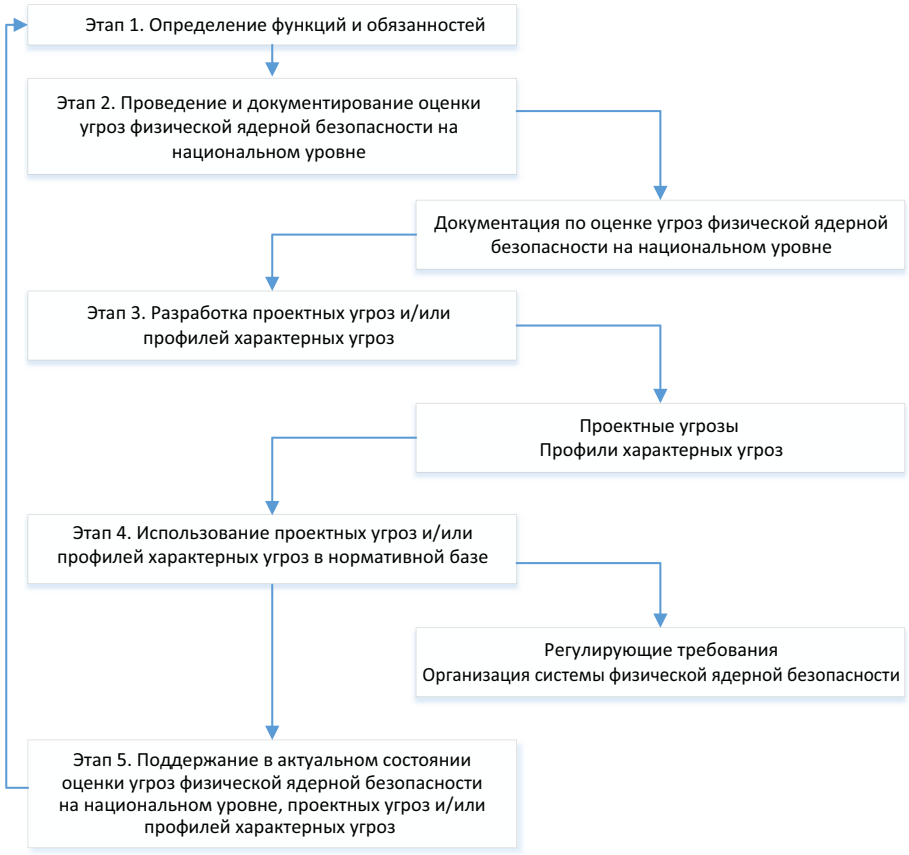


РИС. 1. Процесс разработки, использования и поддержания в актуальном состоянии оценки угроз физической ядерной безопасности на национальном уровне и соответствующей документации, а также проектных угроз и профилей характерных угроз.

4) использование моделей проектной угрозы и/или профилей характерных угроз в рамках нормативно-правовой базы;
5) поддержание в актуальном состоянии оценки угроз физической ядерной безопасности на национальном уровне, проектных угроз и/или профилей характерных угроз.

3.2. На этапе 1 государству следует определить функции и обязанности, которые согласно нормативно-правовой базе государства в этом процессе выполняют регулирующий орган и другие компетентные органы, а также операторы.

3.3. На этапе 2 — проведение оценки угроз физической ядерной безопасности на национальном уровне — компетентному органу, ответственному за проведение этой оценки, следует совместно с другими соответствующими компетентными органами собрать оперативную информацию и другую информацию об угрозах, включая информацию из открытых источников, о прошлых событиях, связанных с физической ядерной безопасностью, равно как и о связанных с безопасностью событиях, не относящихся к ядерной деятельности. Компетентным органам следует проанализировать собранную информацию и оценить ее потенциальную значимость с точки зрения физической ядерной безопасности. Компетентным органам следует также оценить достоверность информации об угрозах и исключить информацию, которая не заслуживает доверия. На основании оставшейся информации компетентным органам следует выявить потенциальных злоумышленников, охарактеризовать вероятность возможных действий злоумышленника и определить признаки и характеристики потенциальных злоумышленников. Наконец, компетентным органам следует оценить, сообразуются ли конкретные возможности злоумышленника с потенциальными целями. Результаты этого процесса следует закрепить в документации по оценке угроз физической ядерной безопасности на национальном уровне.

3.4. В рамках этапа 3 компетентному органу, ответственному за разработку профилей характерных угроз, при необходимости по согласованию с другими компетентными органами следует разработать, используя результаты оценки угроз физической ядерной безопасности на национальном уровне, модели проектной угрозы для конкретного материала, установки или вида деятельности и/или разработать профили характерных угроз, применимые к различным видам и категориям ядерного материала, другого радиоактивного материала, связанных с ним установок и видов деятельности.

3.5. Действия регулирующего органа на этапе 4 будут зависеть от применяемого подхода к регулированию:

а) при подходе, ориентированном на достижение определенных показателей, регулирующему органу следует довести информацию о проектных угрозах до сведения соответствующих операторов, которые затем должны разработать сценарии нападения в контексте конкретных установок и использовать эти сценарии при проектировании систем физической ядерной безопасности для противодействия проектным угрозам и достижения закрепленных в законодательной базе государства целей физической ядерной безопасности;

b) при предписывающем подходе регулирующему органу следует разработать требования к нормативному регулированию на основе профилей характерных угроз и установленных в законодательной базе государства целей физической ядерной безопасности и обеспечить, чтобы операторы применяли на практике системы и меры физической ядерной безопасности в соответствии с этими требованиями;

c) при использовании комбинированного подхода регулирующему органу следует включить элементы, почерпнутые из обоих подходов — подхода, ориентированного на достижение определенных показателей, и предписывающего подхода.

3.6. На этапе 5 компетентным органам следует проанализировать и при необходимости пересмотреть оценку угроз физической ядерной безопасности на национальном уровне и документацию к ней, проектные угрозы и/или профили характерных угроз. Решение о необходимости пересмотреть эти документы может быть принято с учетом определенного цикла рассмотрения, а также в случае изменений во внешней среде, откуда исходят угрозы, и/или с целью учесть уроки, выявленные после события, связанного с физической ядерной безопасностью. Если новые и зарождающиеся угрозы требуют немедленного рассмотрения, компетентным органам следует совместно с операторами предпринять необходимые действия для реагирования на эти угрозы — и если потребуется, то независимо от имеющихся проектных угроз или профилей характерных угроз, до того как последние будут пересмотрены. Этот процесс следует предусмотреть в качестве элемента государственного режима физической ядерной безопасности.

3.7. Каждый из перечисленных выше этапов рассматривается более подробно в разделах 4–8, где изложены, в частности, более конкретные указания для государств, компетентных органов и операторов касательно реализации этих этапов на практике.

4. ФУНКЦИИ И ОБЯЗАННОСТИ

4.1. Функции и обязанности, связанные с оценкой угроз физической ядерной безопасности на национальном уровне и разработкой проектной угрозы и/или профилей характерных угроз, распределяются между государством, соответствующими компетентными органами (включая регулирующий орган) и операторами. Эти функции и обязанности следует

четко определить до начала работы по оценке угроз физической ядерной безопасности на национальном уровне.

ГОСУДАРСТВО

4.2. В сферу ответственности государства входит назначение, координация и контроль работы компетентных органов, которые управляют следующими видами деятельности либо принимают в ней участие:

a) выполнение оценки угроз физической ядерной безопасности на национальном уровне и поддержание в актуальном состоянии этой оценки и документирования ее результатов;
b) разработка и поддержание в актуальном состоянии моделей проектной угрозы и/или профилей характерных угроз;
c) использование моделей проектной угрозы и/или профилей характерных угроз[4].

4.3. Событие, связанное с физической ядерной безопасностью, может привести к возникновению ядерной или радиологической аварийной ситуации. В пункте 4.22 публикации Серии норм безопасности МАГАТЭ, № GSR Part 7, «Готовность и реагирование в случае ядерной или радиологической аварийной ситуации» [11] говорится, что «правительство должно обеспечивать, чтобы оценка опасностей включала рассмотрение результатов оценок угроз, проведенных для целей физической ядерной безопасности».

КОМПЕТЕНТНЫЕ ОРГАНЫ

4.4. Необходимо, чтобы в процессе оценки угроз физической ядерной безопасности на национальном уровне принимали участие все соответствующие компетентные органы, что позволит выявить и учесть как можно более полный спектр достоверных угроз.

4.5. Экспертными знаниями, необходимыми для выявления и оценки достоверных угроз, могут располагать несколько организаций в государстве, такие как разведывательные организации (включая спецслужбы),

[4] Государство может назначать различные компетентные органы в качестве кураторов тех или иных процессов, однако их функции и обязанности должны быть четко определены, а механизм координации между компетентными органами должен быть хорошо налажен и функционировать.

министерства внутренних и иностранных дел, центры компьютерной безопасности, правоохранительные органы, военные службы, регулирующий орган по физической ядерной безопасности и другие соответствующие организации. В таких организациях есть сотрудники, знакомые с процессами сбора и анализа информации и обладающие навыками для дачи необходимых заключений. Кроме того, такие организации могут обладать доступом к определенным источникам информации, включая информацию, полученную в результате контактов с другими государствами или региональными или международными организациями.

4.6. К обязанностям компетентных органов может относиться следующее:

a) сбор и обобщение информации о потенциальных угрозах;
b) анализ имеющейся информации об угрозах в целях обеспечения ее достоверности;
c) обмен актуальной информацией об угрозах с другими компетентными органами;
d) координация действий с другими компетентными органами с целью определить круг достоверных угроз, которые имеют отношение к физической ядерной безопасности;
e) сотрудничество в процессе оценки угроз, выявление потенциальных злоумышленников и документирование оценки угроз физической ядерной безопасности на национальном уровне;
f) разработка моделей проектной угрозы и/или профилей характерных угроз исходя из результатов оценки угроз физической ядерной безопасности на национальном уровне;
g) поддержание в актуальном состоянии оценки угроз физической ядерной безопасности на национальном уровне и соответствующей документации, а также моделей проектной угрозы и профилей характерных угроз;
h) при необходимости — обмен документацией по оценке угроз физической ядерной безопасности на национальном уровне с соответствующими организациями, осуществляющими аварийное реагирование[5];

[5] Во избежание неверного толкования в данной публикации используется термин «организация, осуществляющая аварийное реагирование», поскольку реагирование в области физической ядерной безопасности подразумевает реагирование на событие, связанное с физической ядерной безопасностью. «Организация, осуществляющая аварийное реагирование» соответствует определению «организации, осуществляющей реагирование», которое закреплено в публикации GSR Part 7 [11].

i) учет результатов оценки угроз физической ядерной безопасности на национальном уровне при оценке опасностей [12];
j) учет аспектов информационной безопасности.

4.7. Сфера ответственности некоторых компетентных органов в государстве (например, национальных и местных органов полиции, вооруженных сил, органов пограничного контроля и таможенных органов) гораздо шире и может включать в себя как самостоятельную, так и совместную с другими органами деятельность по защите от угроз, связанных с физической ядерной безопасностью. В ответственность некоторых компетентных органов может также входить оказание помощи оператору во время события, связанного с физической ядерной безопасностью. Таким компетентным органам следует принимать участие либо оказывать консультативную помощь в процессе разработки моделей проектной угрозы и/или профилей характерных угроз, а также регулирующих требований.

4.8. Регулирующий орган по физической ядерной безопасности, при необходимости координируя свою деятельность с другими компетентными органами, отвечает за выполнение следующих задач:

a) разработка предписывающих требований для операторов на основе профилей характерных угроз и/или предоставление операторам моделей проектной угрозы и требований, ориентированных на достижение определенных показателей, для использования при определении сценариев нападений и разработке систем и мер физической ядерной безопасности;
b) обеспечение того, чтобы операторы анализировали и при необходимости пересматривали меры физической безопасности и противоаварийные меры с учетом разработанных сценариев нападений и результатов оценки угроз.

ОПЕРАТОРЫ

4.9. Операторам следует применять в своей практике системы и меры физической ядерной безопасности, отвечающие одному или всем перечисленным ниже условиям:

a) соответствуют нормативным требованиям, включая соответствующие предписывающие требования, разработанные на основе профилей характерных угроз;

b) обеспечивают защиту при различных сценариях нападения, которые разработаны на основе проектной угрозы с учетом особенностей конкретных установок или видов деятельности.

4.10. В отдельных случаях распределение ответственности за применение мер физической ядерной безопасности между операторами и компетентными органами может быть обусловлено компетенциями операторов в части учета влияния конкретных мер физической ядерной безопасности на финансовые и эксплуатационные аспекты, а также на техническую безопасность. При разработке моделей проектной угрозы, профилей характерных угроз и нормативных требований следует принимать во внимание как официальную, так и неофициальную информацию, которую предоставляют операторы. В частности, операторам следует предоставить следующее:

a) информацию о связанных с физической ядерной безопасностью угрозах конкретным установкам или видам деятельности, которые необходимо рассмотреть на предмет включения в проектную угрозу и/или профили характерных угроз;
b) замечания и комментарии для регулирующего органа касательно влияния потенциальных решений, касающихся проектной угрозы, профилей характерных угроз и/или нормативных требований, на финансовые и эксплуатационные аспекты, а также на техническую безопасность и физическую безопасность, если это будет сочтено необходимым и требоваться в соответствии с нормативно-правовой базой;
c) вспомогательную информацию о сценариях нападений и признаках и характеристиках злоумышленников, которая может быть получена в результате изучения имевших место физических нападений, кибератак и «смешанных» нападений, если это будет сочтено необходимым и требоваться в соответствии с нормативно-правовой базой.

5. ПРОВЕДЕНИЕ ОЦЕНКИ УГРОЗ ФИЗИЧЕСКОЙ ЯДЕРНОЙ БЕЗОПАСНОСТИ НА НАЦИОНАЛЬНОМ УРОВНЕ

5.1. Цель оценки угроз физической ядерной безопасности на национальном уровне — обеспечить оценку достоверных угроз, описать мотивы, намерения и возможности потенциальных злоумышленников. В ее задачу не входит описание конкретных сценариев нападения.

5.2. Достаточно подробное и конкретное описание потенциальных угроз может быть использовано для определения уровня защиты, подходящего и достаточного для ядерного материала и другого радиоактивного материала, а также связанных с ним установок и видов деятельности, и закладывает основу для создания системы физической ядерной безопасности.

5.3. В процессе оценки угроз физической ядерной безопасности на национальном уровне происходит сбор и анализ информации о существующих угрозах и потенциальных угрозах достоверного характера, а также сбор и обобщение информации о признаках и характеристиках потенциальных злоумышленников. Результаты оценки угроз физической ядерной безопасности на национальном уровне представляют собой подробное описание угроз, связанных с физической ядерной безопасностью, и оформляются в виде документации по оценке угроз физической ядерной безопасности на национальном уровне. Чтобы собрать и проанализировать эту информацию, необходимо тесное взаимодействие всех соответствующих организаций, имеющих разные области специализации и сферы ответственности. Залогом эффективности работы по оценке угроз физической ядерной безопасности на национальном уровне являются тесные рабочие отношения между всеми соответствующими организациями. Чтобы поддерживать актуальность такой оценки, для облегчения процесса периодического анализа и пересмотра результатов следует вести отчетность о проведении оценки угроз физической ядерной безопасности на национальном уровне.

5.4. В разделе 4 приводится описание функций и обязанностей, связанных с выполнением либо обеспечением выполнения работ, о которых подробно рассказывается в следующих подразделах.

ВВОДНЫЕ ДАННЫЕ: СБОР РЕЛЕВАНТНОЙ ИНФОРМАЦИИ ОБ УГРОЗАХ

5.5. Первоочередной задачей процесса оценки угроз физической ядерной безопасности на национальном уровне является сбор и обобщение исчерпывающей информации обо всех потенциальных злоумышленниках, их мотивах, намерениях и возможностях. Эта информация может включать как конфиденциальные, так и неконфиденциальные сведения и должна охватывать не только физические, но и связанные с информационными технологиями возможности, которыми могут располагать как потенциальные инсайдеры, так и внешние злоумышленники.

5.6. Следует определить потенциальные источники информации и организовать сбор релевантной информации. При этом необходимо принимать во внимание вопрос конфиденциальности информации, чтобы обеспечить надлежащую безопасность как самой информации, так и ее источников. В случае отсутствия механизма обмена информацией об угрозах между всеми участвующими в процессе оценки угроз организациями следует создать такой механизм, который будет обеспечивать безопасности конфиденциальной информации. Создание механизмов обмена информацией об угрозах может потребовать заключения письменных соглашений.

5.7. Достаточную информацию для разработки системы физической ядерной безопасности могут обеспечить разведывательные данные и другие источники информации. Однако в связи с ограниченностью разведывательных данных и динамичным характером угроз те системы физической ядерной безопасности, которые разработаны лишь с учетом известных на сегодняшний день угроз, перед лицом будущих угроз могут оказаться неэффективными.

5.8. При оценке угроз физической ядерной безопасности на национальном уровне не следует опираться лишь на единственный источник информации. Наиболее полную, достоверную и надежную оценку угроз физической ядерной безопасности на национальном уровне обеспечит использование разведывательной информации и информации об угрозах из нескольких источников, обобщаемой в рамках единой целостной оценки. При сборе данных следует принимать во внимание все национальные и международные источники достоверных и актуальных разведывательных данных и информации об угрозах.

5.9. В число источников информации и разведывательных данных при необходимости следует включать разведывательные организации (включая спецслужбы), организации в сфере компьютерной и информационной безопасности, правоохранительные органы, Международную организацию уголовной полиции, регулирующий орган по физической ядерной безопасности и другие компетентные органы, таможенные и пограничные службы, вооруженные силы, грузоотправителей и перевозчиков, а также официальную государственную отчетность, отчеты операторов по инцидентам, базы данных международных организаций и другие открытые источники.

5.10. Источниками дополнительной информации о потенциальных угрозах, в особенности угрозах компьютерной безопасности, могут служить

организации научно-технической поддержки, коммерческие структуры и открытые базы данных. Информацией о таких угрозах, их признаках и характеристиках могут располагать также операторы.

5.11. В целях установления возможных аналогий с угрозами физической ядерной безопасности следует рассматривать релевантную информацию о признаках и характеристиках потенциальных угроз, применимых к другим типам критически важной инфраструктуры.

5.12. Следует собирать информацию о недавних и имевших место в прошлом событиях, связанных с физической ядерной безопасностью (включая события, связанные с компьютерной безопасностью), если таковые случались.

5.13. Необходимо, чтобы сбор информации был направлен на выявление всех актуальных типов угроз, включая:

a) глобальные, национальные и локальные угрозы;
b) физические нападения, кибератаки и «смешанные» нападения;
c) инсайдерские угрозы, действия внешних злоумышленников и угрозы, возникающие в результате сговора инсайдеров и внешних злоумышленников.

5.14. Следует также принимать в расчет реальные возможности злоумышленника, даже если они не были продемонстрированы. Кроме того, следует уделять внимание таким аспектам, как упорство потенциальных злоумышленников, которые могут планировать совершение многоэтапных нападений в течение длительного времени, возможные технологические разработки, потенциальная частота нападений и возможность атак, затрагивающих цепь поставок (например, взлом аппаратного оборудования и/или модифицирование программного обеспечения перед поставкой).

АНАЛИЗ РЕЛЕВАНТНОЙ ИНФОРМАЦИИ ОБ УГРОЗАХ

5.15. После того как сбор релевантной информации об угрозах завершен, ее следует обобщить с использованием инструментов управления информацией, чтобы составить предметный указатель и классифицировать информацию, прежде чем приступать к ее анализу. Упорядочивание должным образом всех разведывательных данных и другой доступной информации является залогом того, что вся необходимая информация будет доступна

для анализа. Затем собранную информацию следует проанализировать, чтобы выявить и задокументировать имеющие отношение к физической ядерной безопасности достоверные мотивы, намерения и возможности потенциальных злоумышленников.

5.16. От полноты собранной информации и точности анализа будет зависеть, насколько можно будет доверять моделям проектной угрозы и/или профилям характерных угроз, составленным в результате этого процесса.

5.17. Сбор и анализ информации в большинстве случаев носит итеративный характер. В процессе анализа часто возникает необходимость в получении дополнительной информации либо выявляются ранее неизвестные или зарождающиеся угрозы, в отношении которых, в свою очередь, требуется информация. Анализ информации об угрозах предусматривает оценку того, что уже известно на основании этой информации, а также формирование суждений о том, как признаки и характеристики злоумышленников могут измениться в будущем.

5.18. В процессе анализа следует оценивать достоверность информации, которая используется в оценке угроз физической ядерной безопасности на национальном уровне. В целом при оценке достоверности информации об угрозах важно принимать во внимание как благонадежность, так и техническую компетентность источника информации. Правоохранительные органы и разведывательные организации, включая спецслужбы, должны указывать степень, в которой, по их мнению, предоставляемая ими информации заслуживает доверия. Полезной может также оказаться легкодоступная информация из открытых источников (например, СМИ или социальных сетей), однако ее точность требует тщательной проверки. При принятии решения о том, каким образом та или иная информация будет использоваться в дальнейшем, следует принимать в расчет степень ее достоверности. Кроме того, при оценке достоверности информации некоторые ее фрагменты могут исключаться как не имеющие отношения к анализу, при этом возможно выявление дополнительных пробелов в информации (например, если информация, предназначенная для восполнения пробелов, будет признана недостаточно достоверной).

5.19. В процессе оценки угроз физической ядерной безопасности на национальном уровне следует уделить внимание рассмотрению как минимум следующих признаков и характеристик злоумышленников в отношении каждой из выявленных угроз (впрочем, соответствующие данные могут

быть доступны не по всем перечисленным признакам и характеристикам в отношении всех угроз):

a) мотивы злоумышленника, которые могут быть, например, политическими, финансовыми, идеологическими и/или личными (например, вследствие недовольства или принуждения);
b) упорство злоумышленника;
c) самоотверженность злоумышленника, включая степень неприятия риска и готовность подвергнуть риску собственную жизнь;
d) продемонстрированные возможности злоумышленника, в том числе характеризация имевших место в прошлом событий, связанных с физической ядерной безопасностью;
e) намерения злоумышленника, такие как саботаж (диверсия) в отношении материала или установки, несанкционированное изъятие ядерного или другого радиоактивного материала, хищение конфиденциальной информации;
f) количество злоумышленников в группе, включая исполнителей атаки, координаторов, а также участников, обеспечивающих вспомогательные функции;
g) виды и число единиц оружия, имеющегося в распоряжении злоумышленника;
h) виды и количество имеющихся в распоряжении злоумышленника взрывчатых веществ, как полученных в виде готовых устройств, так и самодельных, а также сложность механизмов их срабатывания;
i) имеющиеся в распоряжении злоумышленника инструменты, такие как механическое, термическое или электромагнитное оборудование, оборудование с ручным или электронным управлением, а также средства связи;
j) имеющийся в распоряжении злоумышленника транспорт, включая его тип (общественный, личный), вид (наземный, морской, воздушный), а также типы и количество транспортных средств;
k) вероятные способы доступа к целям, как физические, так и связанные с информационными технологиями;
l) влияние на операции и/или персонал;
m) тактика потенциального злоумышленника, например скрытность, обман, силовые действия, разведка или социальная инженерия;
n) навыки планирования злоумышленника, например способность спланировать отвлекающий маневр или координировать одновременное нападение небольших групп;
o) практические навыки, знания и опыт злоумышленника, включая навыки в инженерном деле, использовании взрывчатых веществ,

химических веществ и средств связи, а также опыт участия в военных или военизированных формированиях;

p) наличие навыков в области компьютерных технологий и компьютерной безопасности, в частности знание систем управления, мер компьютерной безопасности, реверс-инжиниринга и тестирования уязвимостей, проектирования протоколов связи, социальной инженерии, обфускации исходного кода, перенаправления запросов, сетевого наблюдения и манипуляции трафиком;

q) наличие знаний о цели атаки или доступ к информации о ней, в частности характеристики цели, планировка установки, планы и процедуры действий на площадке, планы безопасности, меры физической безопасности, меры ядерной безопасности и радиационной защиты, операции на установке и при перевозке, возможные точки входа для кибератак, процедуры и планы предоставления услуг поставщиков, а также цепи поставок и закупочные процедуры;

r) источники и объемы финансирования, а также способы его получения;

s) потенциал использования инсайдеров (в том числе путем сговора, принуждения либо обмана), возможное число инсайдеров, а также являются ли инсайдеры пассивными или активными, готовы ли они к насилию или нет;

t) структуры поддержки злоумышленников: наличие или отсутствие местных сторонников, поддерживающих организаций или логистической поддержки.

РЕЗУЛЬТАТ: ДОКУМЕНТАЦИЯ ПО ОЦЕНКЕ УГРОЗ ФИЗИЧЕСКОЙ ЯДЕРНОЙ БЕЗОПАСНОСТИ НА НАЦИОНАЛЬНОМ УРОВНЕ

5.20. Результаты оценки угроз физической ядерной безопасности на национальном уровне фиксируются в виде документации по оценке угроз физической ядерной безопасности на национальном уровне, в которой содержится описание как общей внешней среды, откуда исходят угрозы физической ядерной безопасности, так и всех известных угроз достоверного характера, которые следует принимать во внимание. Это описание обосновывается аналитическими выкладками и должно включать как можно более подробные сведения об угрозах и о степени достоверности информации.

5.21. Документация по оценке угроз физической ядерной безопасности на национальном уровне и информация об источниках разведывательных данных, как правило, подлежит защите в качестве конфиденциальной информации.

6. РАЗРАБОТКА МОДЕЛИ ПРОЕКТНОЙ УГРОЗЫ И ПРОФИЛЕЙ ХАРАКТЕРНЫХ УГРОЗ

6.1. Как было указано в разделе 5, по завершении процесса оценки угроз физической ядерной безопасности на национальном уровне выпускается документация по оценке угроз физической ядерной безопасности на национальном уровне. На основе оценки угроз физической ядерной безопасности на национальном уровне могут разрабатываться профили угроз в виде модели проектной угрозы и/или профилей характерных угроз. Эти профили включают описание достоверно установленных злоумышленников, от действий которых должны быть защищены установки и виды деятельности, в рамках которых имеет место использование или хранение ядерного материала или другого радиоактивного материала, а также признаки и характеристики этих злоумышленников.

ПОДХОДЫ К РЕГУЛИРОВАНИЮ И ПРОФИЛИ УГРОЗ

6.2. В контексте нормативного регулирования эксплуатации установки или конкретного вида деятельности могут применяться три разных подхода: ориентированный на достижение определенных показателей, предписывающий и комбинированный. В рамках подхода, ориентированного на достижение определенных показателей, оператору необходимо разработать и внедрить систему физической ядерной безопасности, обеспечивающую достижение установленных государством целей в области физической ядерной безопасности, принимая при этом во внимание предоставленные регулирующим органом критерии проектной угрозы, требуемый уровень эффективности защиты от злоумышленных действий и порядок реагирования в чрезвычайных ситуациях. В рамках предписывающего подхода регулирующий орган без предоставления оператору информации об угрозах разрабатывает конкретные меры по обеспечению физической ядерной безопасности, которые он счел необходимыми для достижения поставленных целей в области физической ядерной безопасности по каждой категории ядерного материала или другого радиоактивного материала и с учетом возможных уровней радиологических последствий. Результатом этой работы является минимальный набор мер, подлежащих осуществлению на практике оператором. Комбинированный подход включает элементы как предписывающего, так и ориентированного на достижение определенных показателей подходов. Более подробные

сведения о каждом из этих подходов к нормативному регулированию можно найти в документах [13, 14].

6.3. Как указано в пункте 2.10, профили характерных угроз часто используются при разработке предписывающих регулирующих требований в отношении определенного подмножества материалов, видов деятельности и/или установок, которые подлежат защите, тогда как проектные угрозы часто определяются для конкретных установок или видов деятельности. Регулирующему органу необходимо определиться с походом к регулированию и выбрать соответствующие профили характерных угроз и/или проектные угрозы, оптимальные с точки зрения потребностей государства и соответствующие его нормативно-правовой базе. Необходимо, чтобы выбранный регулирующим органом подход прошел согласование в системе государственной власти, так как следует ожидать, что для его реализации регулирующему органу и операторам потребуются определенные ресурсы.

6.4. Использование в качестве основы для разработки систем и мер физической ядерной безопасности проектной угрозы в рамках подхода, ориентированного на достижение определенных показателей, может способствовать эффективному использованию ресурсов, так как при этом становится возможна разработка требований к защите и системам и мерам физической ядерной безопасности, ориентированным на конкретные имеющиеся угрозы, а не на все угрозы в целом. Применение подхода, ориентированного на достижение определенных показателей, наряду с концепцией проектной угрозы позволяет адаптировать проект системы физической ядерной безопасности под конкретные особенности материала, вида деятельности или установки (включая ее систему контроля и управления), а также создать базу для оценки систем и мер физической ядерной безопасности (с возможностью их последующей доработки в случае необходимости) и разработать четкие принципы определения ответственности оператора в сфере физической ядерной безопасности. Помимо этого, использование проектной угрозы закладывает более детальные и точные технические основы для критериев проектирования и оценки, а также дает более высокую степень уверенности в том, что выбранная защита является достаточной.

6.5. Использование проектной угрозы в рамках подхода, ориентированного на достижение определенных показателей, предполагает более высокую потребность в ресурсах и квалифицированных кадрах со стороны регулирующего органа и оператора. В связи с этим при принятии решения

об использовании проектной угрозы может иметь значение наличие необходимых ресурсов и персонала: у регулирующего органа — для формулирования концепции проектной угрозы и у оператора — для ее эффективного использования в процессе разработки систем и мер физической ядерной безопасности. При этом, если государство считает необходимой соответствующую степень уверенности, обусловленную использованием проектной угрозы, оно должно обеспечить наличие необходимых ресурсов и кадров.

6.6. В частности, государствам следует рассмотреть возможность использования проектной угрозы при разработке требований к физической защите ядерного материала и ядерных установок, применимых к случаям несанкционированного изъятия ядерного материала категории 1 и саботажа (диверсии) в отношении ядерного материала и ядерных установок, которые потенциально могут привести к серьезным радиологическим последствиям, если на территории государства имеются подобные материалы или установки [2]. Помимо этого, государствам следует рассмотреть возможность разработки модели проектной угрозы и для других случаев, если они считают, что потенциальные последствия злоумышленного действия будут тяжелыми.

6.7. При защите ядерного материала или другого радиоактивного материала, а также связанных с ними видов деятельности или установок, в отношении которых можно рассчитывать на менее тяжелый характер потенциальных последствий, возможность разработки модели проектной угрозы следует рассмотреть в следующих случаях:

a) исходя из оценки угроз физической ядерной безопасности на национальном уровне, имеется угроза, связанная с выявленным намерением совершить злоумышленное действие;
b) исходя из оценки угроз физической ядерной безопасности на национальном уровне, имеется угроза с большой возможностью ее осуществления, в отношении которой сведения о намерениях отсутствуют;
c) оценка угроз физической ядерной безопасности на национальном уровне характеризуется значительной неопределенностью, обусловленной недостатком данных или ненадежностью их источников.

6.8. Для новых установок государство может рассмотреть целесообразность и долгосрочные преимущества проектирования системы защиты более высокого уровня, чем это необходимо исходя из признаков

и характеристик угроз, выявленных в рамках текущей оценки угроз физической ядерной безопасности на национальном уровне. Это позволит снизить возможные дополнительные затраты на ее доработку после ввода установки в эксплуатацию.

РАЗРАБОТКА МОДЕЛИ ПРОЕКТНОЙ УГРОЗЫ

6.9. Разработка модели проектной угрозы ведется на базе результатов оценки угроз физической ядерной безопасности на национальном уровне, при этом в ходе разработки необходимо решить следующие пять задач:

1) работа с документацией по оценке угроз физической ядерной безопасности на национальном уровне с целью выявления соответствующих угроз с описанием мотивов, намерений и/или возможностей совершения злоумышленного действия;
2) упорядочение и обобщение признаков и характеристик злоумышленников;
3) доработка обобщенных и упорядоченных признаков и характеристик злоумышленников с учетом факторов политики;
4) адаптация признаков и характеристик злоумышленников к условиям конкретных установок и видов деятельности;
5) окончательная доработка модели проектной угрозы.

Работа с документацией по оценке угроз физической ядерной безопасности на национальном уровне

6.10. В рамках этой работы необходимо выявить цели, в случае которых совершение злоумышленных действий может привести к указанным государством неприемлемым радиологическим последствиям. Затем следует рассмотреть эти цели с учетом признаков и характеристик потенциальных злоумышленников, описанных в документации по оценке угроз физической ядерной безопасности на национальном уровне, чтобы определить круг актуальных для этих целей угроз, способных привести к неприемлемым радиологическим последствиям. При этом необходимо также рассмотреть мотивы, намерения и возможности злоумышленников в отношении указанных целей.

6.11. Следует проработать описания злоумышленников, имеющиеся в документации по оценке угроз физической ядерной безопасности на национальном уровне, на предмет определения того, кто из них имеет

возможности для совершения злоумышленного действия, способного привести к неприемлемым радиологическим последствиям. Если какой-либо тип злоумышленника не обладает достаточными для этого возможностями, он может быть исключен из дальнейшего рассмотрения. Однако подобные решения следует принимать с осторожностью. В частности, не следует исключать угрозу из дальнейшего рассмотрения на основании того, что имеющаяся система физической ядерной безопасности представляется достаточной для защиты установки или деятельности от злоумышленников. При оценке возможностей злоумышленников в ходе разработки моделей проектной угрозы не следует принимать в расчет действующие меры по обеспечению физической ядерной безопасности[6].

6.12. Затем следует проанализировать каждый тип злоумышленника, который, как предполагается, обладает достаточными возможностями для совершения злоумышленного действия, способного привести к неприемлемым радиологическим последствиям, на предмет предполагаемого наличия мотивов и намерений, достаточных для совершения этого действия. При отсутствии достаточных мотивов и намерений данный тип злоумышленника может быть исключен из дальнейшего рассмотрения. Однако необходимо проявлять осторожность при принятии решения об исключении того или иного типа, обладающего достаточными возможностями, только исходя из отсутствия выявленных мотивов и намерений. При принятии решения об исключении того или иного типа злоумышленника следует изучить соображения в отношении того, соответствуют ли выявленные мотивы злоумышленника потенциальным последствиям такого злоумышленного действия и достаточно ли достоверны данные, на основе которых оценивались эти мотивы и намерения.

6.13. Причины исключения того или иного типа злоумышленника, описанного в документации по оценке угроз физической ядерной безопасности на национальном уровне, из дальнейшего рассмотрения в рамках разработки модели проектной угрозы должны тщательно документироваться. В случае появления новой информации, значимой в

[6] Это условие специально сделано настолько строгим. Например, меры по обеспечению физической ядерной безопасности могут быть позднее отменены оператором, если проектная угроза не предполагает такие признаки и характеристики злоумышленника, в отношении которых эти меры принимаются и являются эффективными.

контексте такого исключения, каждый исключенный тип злоумышленника должен быть проанализирован повторно.

6.14. Итогом работы с документацией является формирование списка всех достоверно установленных типов злоумышленников, которые имеют соответствующие возможности и могут иметь мотивы и намерения для совершения злоумышленного действия, способного привести к неприемлемым радиологическим последствиям.

Упорядочение и обобщение признаков и характеристик злоумышленника

6.15. Каждый из выявленных в ходе работы с документацией по оценке угроз физической ядерной безопасности на национальном уровне наборов соответствующих признаков злоумышленника должен быть отнесен к надлежащему типу злоумышленника. При этом необходимо разработать описание всех достоверных типов злоумышленника. Для наглядности каждому типу злоумышленника может быть присвоено условное название (например, «террористы», «преступники», «экстремисты»), однако для каждого типа необходимо также определить соответствующие признаки и характеристики. Угроза, представляемая каждым типом злоумышленника, должна соответствовать диапазону признаков и характеристик, имеющихся у тех или иных потенциальных злоумышленников, которые были отнесены к этому типу.

6.16. Необходимо, чтобы соответствующие признаки и характеристики в рамках каждого типа были упорядочены и обобщены. Результатом должен стать не просто набор наиболее ярких признаков и характеристик различных злоумышленников, но их достоверное сочетание, которое в реальности может обнаружиться у конкретного злоумышленника.

Уточнение обобщенных и упорядоченных признаков и характеристик злоумышленника с учетом факторов политики

6.17. Обобщенные и упорядоченные признаки и характеристики необходимо оценить в контексте всех соответствующих выявленных факторов политики. Результатом этой оценки может стать уточнение обобщенных и упорядоченных признаков и характеристик различных типов злоумышленников, необходимое для обеспечения надежного уровня безопасности, а также изменение предполагаемого уровня возможностей злоумышленников.

6.18. Например, обобщенные и упорядоченные признаки и характеристики могут уточняться с учетом того или иного уровня консерватизма, заложенного в оценку угрозы физической ядерной безопасности на национальном уровне. Целью такого уточнения может быть компенсация неопределенности данных, использованных в оценке угрозы физической ядерной безопасности на национальном уровне, а также широты интерпретации этих данных; обеспечение долгосрочной эффективности систем и мер физической ядерной безопасности оператора в условиях меняющейся с течением времени угрозы; учет признаков и характеристик угроз, которые в настоящее время слабо изучены или не изучены, с целью дополнительного повышения уровня безопасности.

6.19. Помимо этого, обобщенные и упорядоченные признаки и характеристики могут уточняться после анализа экономической эффективности. Этот анализ может включать сопоставление пользы для общества, которую приносят потенциальные цели злоумышленных действий, последствий для общества в случае успешного осуществления злоумышленных действий в отношении этих целей, а также затрат, которые лягут на общество в связи с реализацией надлежащих мер физической ядерной безопасности, необходимых для снижения рисков таких действий, в сравнении с затратами на защиту других объектов, для которых имеются риски последствий схожей тяжести (например, взрывоопасные, химические и биологические производства), или другой критической инфраструктуры.

6.20. Также может потребоваться учет других факторов политики, таких как разделение ответственности в сфере физической ядерной безопасности между государством и операторами, влияние решений, касающихся допустимости рисков, на уровень доверия населения, вклад объектов, которые могут являться потенциальными целями злоумышленных действий, в общественное благосостояние (например, сферы применения ядерного материала или радиоактивного материала), уровень доверия соседних государств к системе физической ядерной безопасности конкретного государства и угрозы в соседних государствах.

6.21. Повышенные требования к безопасности и другие отмеченные здесь факторы политики, вероятно, станут основанием для повышения при разработке модели проектной угрозы предполагаемых уровней возможностей, связанных с обобщенными и упорядоченными

характеристиками злоумышленников, тогда как анализ затрат и результатов может способствовать снижению этих уровней.

Адаптация признаков и характеристик злоумышленника к условиям конкретных установок и видов деятельности

6.22. Обобщенные признаки и характеристики злоумышленника, доработанные с учетом факторов политики, необходимо адаптировать к условиям конкретных установок и видов деятельности. В случае конкретных установок могут иметь значение их местоположение и доступность, особенности их конструкции и эксплуатации, а также наличие тех или иных местных угроз. В случае конкретных видов деятельности целесообразно обратить внимание на технические регламенты, режимы и маршруты транспортировки, а также те или иные угрозы, характерные для конкретных местоположений и маршрутов.

Окончательная доработка модели проектной угрозы

6.23. Прежде чем включать проектную угрозу в нормативно-правовую базу регулирования, следует рассмотреть замечания других компетентных органов и заинтересованных сторон. Окончательное решение о содержании модели проектной угрозы и общей ответственности за это содержание должно приниматься компетентным органом, который был назначен государством курировать процесс разработки.

6.24. Примерное описание проектной угрозы приводится в дополнении.

РАЗРАБОТКА ПРОФИЛЕЙ ХАРАКТЕРНЫХ УГРОЗ

6.25. Профили характерных угроз разрабатываются, как и модель проектной угрозы, на основе оценки угрозы физической ядерной безопасности на национальном уровне. При их разработке используется подход, описанный в пунктах 6.9–6.24 для проектной угрозы, однако при этом на каждом этапе обычно используются менее жесткие требования, а число участвующих организаций может быть меньше. Кроме того, адаптировать признаки и характеристики злоумышленников к условиям конкретных установок и видов деятельности не требуется.

6.26. В ходе разработки профилей характерных угроз необходимо решить следующие четыре задачи:

1) работа с документацией по оценке угроз физической ядерной безопасности на национальном уровне с целью выявления соответствующих угроз с описанием мотивов, намерений и/или возможностей совершения злоумышленного действия;
2) упорядочение и обобщение признаков и характеристик злоумышленника в виде их наборов, отражающих определенный диапазон признаков и характеристик;
3) уточнение репрезентативных признаков и характеристик злоумышленника на основе соответствующих соображений политики;
4) окончательная доработка профилей характерных угроз.

УГРОЗЫ, СУЩЕСТВУЮЩИЕ В РАМКАХ И ЗА РАМКАМИ ПРОЕКТНОЙ УГРОЗЫ

6.27. Оценка угроз физической ядерной безопасности на национальном уровне позволяет с высокой вероятностью выявить широкий спектр возможностей злоумышленников. Государству необходимо с учетом известных, имеющихся и преобладающих угроз установить уровень угрозы или возможностей злоумышленников, при превышении которого ответственность за реагирование будет переходить преимущественно к государству, а не оператору, ввиду того что возможности и/или ресурсы оператора в части обеспечения защиты и реагирования могут быть недостаточными с учетом столь широких возможностей злоумышленников и столь тяжелых потенциальных последствий. При этом оператор может оказывать государству определенную помощь в вопросах защиты от этих угроз или смягчения их последствий.

6.28. Таким образом, в рамках разработки модели проектной угрозы следует рассматривать злоумышленников, возможности которых не превосходят этот установленный государством уровень, предполагая при этом, что в случае его превышения основная ответственность за обеспечение защиты и принятие мер реагирования будет лежать не на операторе. Ответственность за противодействие злоумышленникам, возможности которых превышают установленный уровень, ложится главным образом на государство. При установлении такого уровня государству следует также принимать в расчет затраты, эксплуатационные последствия и другие факторы.

7. ИСПОЛЬЗОВАНИЕ ПРОЕКТНОЙ УГРОЗЫ И ПРОФИЛЕЙ ХАРАКТЕРНЫХ УГРОЗ

7.1. Как было указано в пунктах 6.2–6.8, государство может принять решение об использовании одного из следующих подходов к нормативному регулированию: подхода, ориентированного на достижение определенных показателей, предписывающего подхода или комбинированного подхода. В настоящем разделе рассматривается использование проектной угрозы и профилей характерных угроз в рамках каждого из этих подходов.

ПОДХОД К РЕГУЛИРОВАНИЮ, ОРИЕНТИРОВАННЫЙ НА ДОСТИЖЕНИЕ ОПРЕДЕЛЕННЫХ ПОКАЗАТЕЛЕЙ

7.2. В рамках подхода, ориентированного на достижение определенных показателей, основой для разработки, реализации и оценки эффективности систем и мер физической ядерной безопасности являются проектные угрозы и установленные государством цели в области физической ядерной безопасности.

7.3. В ходе использования проектной угрозы в рамках подхода, ориентированного на достижение определенных показателей, необходимо решить следующие задачи.

a) Регулирующему органу следует предоставить операторам критерии проектной угрозы.
b) Каждому оператору следует исходя из предоставленных критериев проектной угрозы совместно с регулирующим органом выявить достоверные сценарии нападений.
c) Каждому оператору следует разработать системы и меры физической ядерной безопасности для конкретной установки или видов деятельности, позволяющие эффективно противостоять нападениям в рамках выявленных сценариев.
d) Каждому оператору следует описать в своем плане обеспечения безопасности устройство используемой им системы физической ядерной безопасности и при необходимости направить этот план в регулирующий орган на утверждение.
e) Регулирующему органу следует оценить эффективность систем физической ядерной безопасности каждого оператора исходя из

сведений об их устройстве, содержащихся в полученных планах обеспечения безопасности.

f) После утверждения плана обеспечения безопасности оператор может приступить к эксплуатации установки или осуществлению соответствующей деятельности.

7.4. Необходимо, чтобы соответствующие организации, ответственные за аварийное реагирование, включая регулирующий орган и оператора, использовали результаты оценки угроз физической ядерной безопасности на национальном уровне в своем анализе опасностей с целью предусмотреть надлежащие меры аварийного реагирования для обеспечения готовности и реагирования в случае ядерной или радиационной аварийной ситуации, которая была обусловлена событием, связанным с физической ядерной безопасностью, и для скоординированного и комплексного реагирования в чрезвычайных ситуациях.

ПРЕДПИСЫВАЮЩИЙ ПОДХОД К РЕГУЛИРОВАНИЮ

7.5. В рамках предписывающего подхода регулирующему органу следует разработать предписывающие нормативные требования, используя для этой цели профили характерных угроз, применимые к каждой категории материала, каждому типу установки и каждому виду деятельности, и исходя из установленных государством целей в области физической ядерной безопасности. Необходимо, чтобы предписывающие требования регулирующего органа указывали системы и меры физической ядерной безопасности, которые необходимо внедрить для обеспечения защиты, достаточной для достижения целей государственного режима физической ядерной безопасности. Руководящие указания, которые могут быть полезны государствам при разработке этих предписывающих нормативных требований, содержатся в документах [13–16].

7.6. В ходе использования профилей характерных угроз в рамках предписывающего подхода необходимо решить следующие задачи.

a) Регулирующему органу следует выявить вероятные сценарии нападений исходя из каждого отдельного профиля характерной угрозы, после чего разработать меры физической ядерной безопасности для различных категорий материалов, типов установок и видов деятельности.

b) Регулирующему органу следует рассмотреть меры, рекомендуемые или предлагаемые в соответствующих публикациях МАГАТЭ, например в документах [2, 3, 9, 13–16], насколько это применимо, и выяснить, позволяют ли эти меры достичь целей в области физической ядерной безопасности или же для того, чтобы обеспечить необходимый в свете соответствующего профиля характерной угрозы уровень защиты, потребуются дополнительные меры.
c) Регулирующему органу следует разработать предписывающие нормативные требования, касающиеся применения на практике предусмотренных мер физической ядерной безопасности.
d) Операторам следует внедрить меры физической ядерной безопасности, предусмотренные соответствующими нормативными требованиями.

КОМБИНИРОВАННЫЙ ПОДХОД

7.7. Как было указано в пункте 6.2 и документах [13, 14], комбинированный подход к нормативному регулированию сочетает элементы предписывающего подхода и подхода, ориентированного на достижение определенных показателей.

7.8. Государство может использовать подход, ориентированный на достижение определенных показателей, в контексте тех установок и видов деятельности, для которых это экономически целесообразно, например в случаях, когда ввиду тяжести возможных последствий события, связанного с физической ядерной безопасностью, необходим повышенный уровень безопасности. Предписывающий подход может использоваться в случае материала, а также связанных с ним установок и видов деятельности, когда возможные последствия события, связанного с физической ядерной безопасностью, представляются не столь тяжелыми. Государство также может использовать подход, ориентированный на достижение определенных показателей, для защиты от одних угроз, а предписывающий подход — от других.

РАЗРАБОТКА СЦЕНАРИЕВ НАПАДЕНИЯ

7.9. Сценарии нападения разрабатываются исходя из представлений о том, как признаки и характеристики злоумышленника могут обусловливать возможность совершения злоумышленного действия, а также могут ли

различные злоумышленники объединить свои усилия для совершения такого действия и каким образом они могут это сделать.

7.10. Сценарий нападения представляет собой постулируемый или предполагаемый набор условий и событий, обычно используемый в рамках анализа или оценки для представления возможных будущих условий или событий, которые необходимо смоделировать, таких как возможное событие, связанное с физической ядерной безопасностью. Сценарий может представлять условия в определенный момент времени или единичное событие, а также отражать изменение условий или развитие событий во времени (включая протекание каких-либо процессов), которые могут привести к событию, связанному с физической ядерной безопасностью, или последовать за ним, включая возможные отдаленные последствия.

7.11. Необходимо, чтобы сценарии нападения включали все вероятные сочетания признаков и характеристик злоумышленника, предусмотренные в профиле характерной угрозы или в модели проектной угрозы, включая сговор между внутренними и внешними злоумышленниками, а также сочетание физического нападения и кибератаки. В сценариях нападения должны быть обозначены: a) вероятные маршруты злоумышленника, b) время проникновения исходя из предполагаемой тактики нападения и сроки принятия мер физической и компьютерной безопасности, c) вероятность обнаружения исходя из наличия датчиков и мер контроля, а также предполагаемая тактика уклонения от них и их преодоления.

7.12. В числе прочего следует рассмотреть сценарии нападения, включающие кибератаки. Кибератака как таковая с крайне малой вероятностью может привести к несанкционированному изъятию материала, однако она может помешать применению мер физической ядерной безопасности, предусмотренных на случай несанкционированного изъятия и саботажа или диверсии, целью которых является предотвращение, обнаружение и задержка таких действий, а также реагирование на них. Помимо этого, кибератака может в той или иной степени препятствовать выполнению функций безопасности и физической ядерной безопасности, учета и контроля ядерного материала, а также готовности и реагирования в случае аварийных ситуаций, тем самым способствуя совершению нападения.

7.13. Целесообразность совершения нападения определяется его сложностью; количеством и техническим уровнем используемых инструментов и других ресурсов; навыками и способностями

злоумышленников; наличием у злоумышленников информации об установке и контрольно-пропускных пунктах (в том числе о местах, где могут быть спрятаны люди и инструменты, и о слабых местах в системах, которые могут быть использованы); общим количеством внешних злоумышленников; возможностями сил реагирования; количеством и характеристиками внутренних злоумышленников (инсайдеров), а также степенью их вовлеченности; эффективностью физических барьеров, мер компьютерной безопасности и средств обнаружения и контроля.

8. ПОДДЕРЖАНИЕ В АКТУАЛЬНОМ СОСТОЯНИИ И ПЕРЕСМОТР ОЦЕНКИ УГРОЗ ФИЗИЧЕСКОЙ ЯДЕРНОЙ БЕЗОПАСНОСТИ НА НАЦИОНАЛЬНОМ УРОВНЕ И СООТВЕТСТВУЮЩЕЙ ДОКУМЕНТАЦИИ, А ТАКЖЕ ПРОФИЛЕЙ УГРОЗ

8.1. Следует периодически проводить анализ документации по оценке угроз физической ядерной безопасности на национальном уровне с целью удостовериться в том, что содержащаяся в ней оценка отражает всеобъемлющую и сбалансированную картину достоверных угроз физической ядерной безопасности в государстве. При необходимости эта оценка должна пересматриваться.

8.2. Анализ (и при необходимости пересмотр) проектных угроз и профилей характерных угроз может быть необходим в случае пересмотра документации по оценке угроз физической ядерной безопасности на национальном уровне, при изменении факторов политики, а также при накоплении опыта в сфере проектирования и оценки систем и мер физической ядерной безопасности или получении нового опыта после события, связанного с физической ядерной безопасностью.

8.3. Анализ оценки угроз физической ядерной безопасности на национальном уровне, проектных угроз и профилей характерных угроз может выполняться, например, с периодичностью в 12–18 месяцев. При этом следует руководствоваться процедурой проведения оценки угроз физической ядерной безопасности на национальном уровне.

8.4. В рамках анализа оценки угроз физической ядерной безопасности на национальном уровне могут рассматриваться новые и меняющиеся угрозы и возможности, для которых отсутствуют сведения об их непосредственной связи с физической ядерной безопасностью, с целью выявления какого бы то ни было возможного влияния этих угроз на безопасность ядерного материала, другого радиоактивного материала и соответствующих установок и видов деятельности.

8.5. В ряде случаев может возникнуть необходимость во внеплановом анализе оценки угроз физической ядерной безопасности на национальном уровне, проектных угроз и профилей характерных угроз. К числу условий и событий, которые могут свидетельствовать о необходимости такого анализа, относятся следующие.

a) Любое событие или действие на территории государства или за ее пределами, непосредственно или косвенно связанное с ядерным материалом, другим радиоактивным материалом и соответствующими установками и видами деятельности, которое существенно меняет представления об угрозе физической ядерной безопасности или фактический уровень серьезности этой угрозы.
b) Значительные изменения в государственной политике, законодательстве или международных договоренностях, затрагивающие обязанности компетентных органов или оператора, например изменение механизмов реагирования и обязанностей организаций.
c) Изменения в установках и видах деятельности, связанных с ядерным материалом или другим радиоактивным материалом, которые могут привести к изменению возможных последствий события, связанного с физической ядерной безопасностью, или появлению новых последствий. Среди таких изменений следует отметить, в частности, строительство установки нового типа, использование материала с более высокой степенью обогащения, использование материала в новом технологическом процессе, возвращение высокообогащенного урана в страну происхождения, изменение технологии с целью перехода на материал более низкой категории, а также повышение уровня физической ядерной безопасности.
d) Предложение о проведении анализа со стороны компетентного органа, организации технической или научной поддержки либо оператора.

8.6. Анализ может показать, что необходимость пересмотра оценки угроз физической ядерной безопасности на национальном уровне, проектных угроз и профилей характерных угроз отсутствует. Однако если анализ

показывает, что оценка угроз физической ядерной безопасности на национальном уровне не отражает должным образом все достоверные угрозы, включая новые и формирующиеся угрозы, данная оценка и соответствующая документация должны быть пересмотрены с привлечением всех соответствующих организаций. В случае значимых и фундаментальных изменений в оценке необходим также пересмотр проектных угроз и профилей характерных угроз.

РЕАГИРОВАНИЕ НА НОВЫЕ И ФОРМИРУЮЩИЕСЯ УГРОЗЫ

8.7. Безотносительно к необходимости регулярного проведения анализа возможно возникновение ситуаций, указывающих на наличие или предполагаемое наличие у злоумышленников новых и непредвиденных физических или связанных с информационными технологиями возможностей, которые представляют достаточную угрозу с точки зрения того, чтобы потребовалось немедленное реагирование на них со стороны государства. Соответствующие сведения могут поступить как через официальные, так и через неофициальные каналы.

8.8. Регулирующему органу и другим компетентным органам следует, помимо процедуры разработки и пересмотра моделей проектной угрозы и профилей характерных угроз, предусмотреть процедуру распространения поступивших сведений об угрозах среди компетентных органов и соответствующих операторов. Эта процедура особенно важна в условиях быстрого изменения уровня серьезности угрозы, когда полный пересмотр оценки угроз физической ядерной безопасности на национальном уровне невозможен из-за нехватки времени.

8.9. Если оператор получает информацию о таком изменении уровня серьезности угрозы по неофициальным каналам, ему следует проинформировать об этом регулирующий орган или другие компетентные органы в установленном порядке, чтобы они имели возможность оценить достоверную вероятность, актуальность и тяжесть возможных последствий этого изменения и определить, какие меры реагирования и в какие сроки необходимо принять государству и/или оператору.

8.10. Дополнительная защита в подобных ситуациях может быть обеспечена путем создания системы заранее определенных уровней повышенной угрозы и соответствующих им заранее определенных комплексов дополнительных мер физической ядерной безопасности, которые вводятся в действие оператором на каждом уровне повышенной угрозы.

Дополнение

ПРИМЕРНОЕ ОПИСАНИЕ ПРОЕКТНОЙ УГРОЗЫ

А.1. Таблица 1 представляет собой пример того, как признаки и характеристики злоумышленника могли бы учитываться при определении проектной угрозы.

А.2. Для составления профилей характерных угроз можно использовать как аналогичный формат (как правило, с меньшей степенью детализации), так и менее формализованный формат.

ТАБЛИЦА 1. ПРИМЕРНЫЙ ПЕРЕЧЕНЬ ПРИЗНАКОВ И ХАРАКТЕРИСТИК ЗЛОУМЫШЛЕННИКА, УЧИТЫВАЕМЫХ ПРИ ОПРЕДЕЛЕНИИ ПРОЕКТНОЙ УГРОЗЫ

	Вооружен	Невооружен
Действие		
Кража[a]	Укажите *да* или *нет*	Укажите *да* или *нет*
Саботаж (диверсия)[b]	Укажите *да* или *нет*	Укажите *да* или *нет*
Общие признаки и характеристики		
Количество	Укажите количество	Укажите количество
Уровень финансирования	Укажите *низкий* или *высокий*	Укажите *низкий* или *высокий*
Инсайдерская поддержка	Укажите *активная* или *пассивная*, а также *насильственная* или *ненасильственная*	Укажите *активная* или *пассивная*, а также *насильственная* или *ненасильственная*
Тактика	Укажите *скрытая* и/или *силовая*	Укажите *скрытая* и/или *силовая*

ТАБЛИЦА 1. ПРИМЕРНЫЙ ПЕРЕЧЕНЬ ПРИЗНАКОВ И ХАРАКТЕРИСТИК ЗЛОУМЫШЛЕННИКА, УЧИТЫВАЕМЫХ ПРИ ОПРЕДЕЛЕНИИ ПРОЕКТНОЙ УГРОЗЫ (продолжение)

	Вооружен	Невооружен
Навыки планирования	Укажите *способность спланировать отвлекающий маневр,* и/или *нападение злоумышленников одновременно небольшими группами,* и/или *знание планировки установки,* и/или *способность спланировать «смешанное» нападение*	Укажите *способность спланировать отвлекающий маневр,* и/или *нападение злоумышленников одновременно небольшими группами,* и/или *знание планировки установки,* и/или *способность спланировать «смешанное» нападение*
Физические признаки и характеристики		
Готовность убить	Укажите *да* или *нет*	Укажите *да* или *нет*
Готовность погибнуть	Укажите *да* или *нет*	Укажите *да* или *нет*
Путь передвижения	Укажите *по воздуху, по автомобильной дороге, по железной дороге, по воде* и/или *под землей*	Укажите *по воздуху, по автомобильной дороге, по железной дороге, по воде* и/или *под землей*
Тип оружия	Укажите *автоматическое оружие*, *полуавтоматическое оружие*, *личное оружие* и/или *ножи*	Неприменимо
Взрывчатое вещество	Укажите тип и количество взрывчатых веществ	Неприменимо
Инструменты	Укажите *электроинструменты*, *ручные инструменты* и/или *инструменты, имеющиеся на площадке*	Укажите *электроинструменты*, *ручные инструменты* и/или *инструменты, имеющиеся на площадке*

ТАБЛИЦА 1. ПРИМЕРНЫЙ ПЕРЕЧЕНЬ ПРИЗНАКОВ И ХАРАКТЕРИСТИК ЗЛОУМЫШЛЕННИКА, УЧИТЫВАЕМЫХ ПРИ ОПРЕДЕЛЕНИИ ПРОЕКТНОЙ УГРОЗЫ (продолжение)

	Вооружен	Невооружен
Технические навыки	Укажите *сложно организованное вторжение с использованием взрывчатых веществ*, *вывод из строя линий связи* и/или *управление оборудованием установки*	Укажите *сложно организованное вторжение с использованием взрывчатых веществ*, *вывод из строя линий связи* и/или *управление оборудованием установки*
Сообщник-инсайдер	Укажите *авторизация доступа*, *сотрудник службы охраны*, *техническое обслуживание оборудования* и/или *лицо, работающее с материалом*	Укажите *авторизация доступа*, *сотрудник службы охраны*, *техническое обслуживание оборудования* и/или *лицо, работающее с материалом*
Признаки и характеристики, относящиеся к операциям в компьютерных сетях		
Программные средства	Укажите *стандартные программные средства*, *вредоносные средства* и/или *средства, разработанные собственными силами*	Укажите *стандартные программные средства*, *вредоносные средства* и/или *средства, разработанные собственными силами*
Экспертные знания и опыт	Укажите *социальная инженерия*, *использование коммерческих средств*, *разработка новых программных средств*, *служебный домен*, *домен управления процессами* и/или *знания об используемой ИТ-системе*	Укажите *социальная инженерия*, *использование коммерческих средств*, *разработка новых программных средств*, *служебный домен*, *домен управления процессами* и/или *знания об используемой ИТ-системе*
Аппаратные средства	Укажите *компьютер*, *мобильный телефон*, *подключение к кабелям* и/или *маршрутизаторам*	Укажите *компьютер*, *мобильный телефон*, *подключение к кабелям* и/или *маршрутизаторам*

ТАБЛИЦА 1. ПРИМЕРНЫЙ ПЕРЕЧЕНЬ ПРИЗНАКОВ И ХАРАКТЕРИСТИК ЗЛОУМЫШЛЕННИКА, УЧИТЫВАЕМЫХ ПРИ ОПРЕДЕЛЕНИИ ПРОЕКТНОЙ УГРОЗЫ (продолжение)

	Вооружен	Невооружен
Способность воздействовать на цепь поставок	Укажите *да* или *нет*	Укажите *да* или *нет*
Упорство злоумышленника	Укажите *способность совершать нападения в течение длительного времени* и/или *повторно*	Укажите *способность совершать нападения в течение длительного времени* и/или *повторно*
Сообщник-инсайдер	Укажите *авторизация доступа*, *управление процессами в СКУ обычным пользователем, администратором* и/или *сторонним поставщиком*	Укажите *авторизация доступа*, *управление процессами в СКУ обычным пользователем, администратором* и/или *сторонним поставщиком*

Примечание. СКУ — системы контроля и управления, ИТ — информационные технологии.

[a] Возможно добавить критерии в отношении количества изъятого материала и/или единоразового либо продолжительного хищения.

[b] Возможно добавить критерии в отношении радиологических последствий.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

[1] 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).

[2] 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).

[3] 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).

[4] 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).

[5] INTERNATIONAL ATOMIC ENERGY AGENCY, Computer Security for Nuclear Security, IAEA Nuclear Security Series No. 42-G, IAEA, Vienna (in preparation).

[6] МЕЖДУНАРОДНОЕ АГЕНТСТВО ПО АТОМНОЙ ЭНЕРГИИ, МЕЖДУНАРОДНАЯ ОРГАНИЗАЦИЯ УГОЛОВНОЙ ПОЛИЦИИ — ИНТЕРПОЛ, Риск-ориентированный подход к мерам физической ядерной безопасности ядерного и другого радиоактивного материала, находящегося вне регулирующего контроля, Серия изданий МАГАТЭ по физической ядерной безопасности, № 24-G, МАГАТЭ, Вена (2024).

[7] Конвенция о физической защите ядерного материала, INFCIRC/274/Rev.1, МАГАТЭ, Вена (1980).

[8] Поправка к Конвенции о физической защите ядерного материала, INFCIRC/274/Rev.1/Mod.1, МАГАТЭ, Вена (2016).

[9] МЕЖДУНАРОДНОЕ АГЕНТСТВО ПО АТОМНОЙ ЭНЕРГИИ, Предупредительные и защитные меры в отношении угроз, исходящих от внутреннего нарушителя, Серия изданий МАГАТЭ по физической ядерной безопасности, № 8-G (Rev. 1), МАГАТЭ, Вена (2020).

[10] МЕЖДУНАРОДНОЕ АГЕНТСТВО ПО АТОМНОЙ ЭНЕРГИИ, Безопасность ядерной информации, Серия изданий МАГАТЭ по физической ядерной безопасности, № 23-G, МАГАТЭ, Вена (2023).

[11] АГЕНТСТВО ПО ЯДЕРНОЙ ЭНЕРГИИ ОЭСР, ВСЕМИРНАЯ МЕТЕОРОЛОГИЧЕСКАЯ ОРГАНИЗАЦИЯ, ВСЕМИРНАЯ ОРГАНИЗАЦИЯ ЗДРАВООХРАНЕНИЯ, ИНТЕРПОЛ, МЕЖДУНАРОДНАЯ МОРСКАЯ ОРГАНИЗАЦИЯ, МЕЖДУНАРОДНАЯ ОРГАНИЗАЦИЯ ГРАЖДАНСКОЙ АВИАЦИИ, МЕЖДУНАРОДНАЯ ОРГАНИЗАЦИЯ ТРУДА, МЕЖДУНАРОДНОЕ АГЕНТСТВО ПО АТОМНОЙ ЭНЕРГИИ, ПАНАМЕРИКАНСКАЯ ОРГАНИЗАЦИЯ ЗДРАВООХРАНЕНИЯ, ПОДГОТОВИТЕЛЬНАЯ КОМИССИЯ ОРГАНИЗАЦИИ ПО ДОГОВОРУ О ВСЕОБЪЕМЛЮЩЕМ ЗАПРЕЩЕНИИ ЯДЕРНЫХ ИСПЫТАНИЙ, ПРОГРАММА ОРГАНИЗАЦИИ ОБЪЕДИНЕННЫХ НАЦИЙ ПО ОКРУЖАЮЩЕЙ СРЕДЕ, ПРОДОВОЛЬСТВЕННАЯ И СЕЛЬСКОХОЗЯЙСТВЕННАЯ ОРГАНИЗАЦИЯ ОБЪЕДИНЕННЫХ НАЦИЙ, УПРАВЛЕНИЕ ОРГАНИЗАЦИИ ОБЪЕДИНЕННЫХ НАЦИЙ ПО КООРДИНАЦИИ ГУМАНИТАРНЫХ ВОПРОСОВ, Готовность и реагирование в случае ядерной или радиологической аварийной ситуации, Серия норм безопасности МАГАТЭ, № GSR Part 7, МАГАТЭ, Вена (2016).

[12] ВСЕМИРНАЯ ОРГАНИЗАЦИЯ ЗДРАВООХРАНЕНИЯ, МЕЖДУНАРОДНАЯ ОРГАНИЗАЦИЯ ТРУДА, МЕЖДУНАРОДНОЕ АГЕНТСТВО ПО АТОМНОЙ ЭНЕРГИИ, ПАНАМЕРИКАНСКАЯ ОРГАНИЗАЦИЯ ЗДРАВООХРАНЕНИЯ, ПРОДОВОЛЬСТВЕННАЯ И СЕЛЬСКОХОЗЯЙСТВЕННАЯ ОРГАНИЗАЦИЯ ОБЪЕДИНЕННЫХ НАЦИЙ, УПРАВЛЕНИЕ ОРГАНИЗАЦИИ ОБЪЕДИНЕННЫХ НАЦИЙ ПО КООРДИНАЦИИ ГУМАНИТАРНЫХ ВОПРОСОВ, Меры по обеспечению готовности к ядерной или радиологической аварийной ситуации, Серия норм безопасности МАГАТЭ, № GS-G-2.1, МАГАТЭ, Вена (2016).

[13] МЕЖДУНАРОДНОЕ АГЕНТСТВО ПО АТОМНОЙ ЭНЕРГИИ, Физическая защита ядерного материала и ядерных установок (практическое применение рекомендаций INFCIRC/225/Revision 5), Серия изданий МАГАТЭ по физической ядерной безопасности, № 27-G, МАГАТЭ, Вена (2022).

[14] INTERNATIONAL ATOMIC ENERGY AGENCY, Security of Radioactive Material in Use and Storage and of Associated Facilities, IAEA Nuclear Security Series No. 11-G (Rev. 1), IAEA, Vienna (2019).

[15] МЕЖДУНАРОДНОЕ АГЕНТСТВО ПО АТОМНОЙ ЭНЕРГИИ, Физическая безопасность радиоактивного материала при перевозке, Серия изданий МАГАТЭ по физической ядерной безопасности, № 9-G, МАГАТЭ, Вена (2023).

[16] INTERNATIONAL ATOMIC ENERGY AGENCY, Security of Nuclear Material in Transport, IAEA Nuclear Security Series No. 26-G, IAEA, Vienna (2015).

ГЛОССАРИЙ

оценка угрозы (threat assessment). Анализ угроз, который выполняется на основе имеющихся разведывательных данных, информации от правоохранительных органов и из открытых источников и в рамках которого рассматриваются мотивы, намерения и возможности, лежащие в основе этих угроз.

проектная угроза (design basis threat). Признаки и характеристики потенциального инсайдера и/или внешних злоумышленников, которые могут предпринять попытку несанкционированного изъятия или саботажа (диверсии) и для противодействия которым создается и оценивается система физической защиты.

профиль угрозы (threat statement). Описание вероятных злоумышленников (включая признаки и характеристики) в виде проектной угрозы или профиля характерной угрозы, которое составляется на основе оценки угроз физической ядерной безопасности на национальном уровне.

профиль характерной угрозы (representative threat statement). Признаки и характеристики потенциального инсайдера и/или внешних злоумышленников, которые могут предпринять попытку несанкционированного изъятия или саботажа (диверсии), предназначенные для использования при разработке предписывающих требований к защите определенных материалов и/или установок.

IAEA
Международное агентство по атомной энергии

№ 27

ЗАКАЗ ПУБЛИКАЦИЙ В СТРАНАХ

Платные публикации МАГАТЭ можно приобрести у нашего основного дистрибьютора или в крупных книжных магазинах. Заказы на бесплатные публикации следует направлять непосредственно в МАГАТЭ.

Заказы на платные публикации

Просьба связаться с местным поставщиком по вашему выбору либо нашим основным дистрибьютором:

Eurospan
1 Bedford Row
London WC1R 4BU
United Kingdom

Торговые заказы и справочная информация:
Тел.: +44 (0)1235 465576
Эл. почта: trade.orders@marston.co.uk

Индивидуальные заказы:
Тел.: +44 (0)1235 465577
Эл. почта: direct.orders@marston.co.uk
www.eurospanbookstore.com/iaea

Дополнительная информация:
Тел.: +44 (0) 207 240 0856
Эл. почта: info@eurospan.co.uk
www.eurospan.co.uk

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

Издательская секция (Publishing Section)
Международное агентство по атомной энергии
Vienna International Centre
PO Box 100
1400 Vienna, Austria
Телефон: +43 1 2600 22529 или 22530
Эл. почта: sales.publications@iaea.org
https://www.iaea.org/ru/publikacii

В настоящей публикации представлена поэтапная методология для оценки угроз физической ядерной безопасности на национальном уровне, включая аспекты физической и компьютерной безопасности, а также для разработки, применения и актуализации моделей проектной угрозы и профилей характерных угроз. Она предназначена для использования государствами, компетентными органами (включая регулирующий орган), соответствующими организациями научно-технической поддержки, а также операторами установок и видов деятельности, связанных с ядерным материалом и другим радиоактивным материалом, включая грузоотправителей и перевозчиков.

МЕЖДУНАРОДНОЕ АГЕНТСТВО ПО АТОМНОЙ ЭНЕРГИИ
ВЕНА