Серия изданий МАГАТЭ по физической ядерной безопасности, № 27-G

Практическое руководство

Физическая защита ядерного материала и ядерных установок (практическое применение рекомендаций INFCIRC/225/Revision 5)

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.

ФИЗИЧЕСКАЯ ЗАЩИТА ЯДЕРНОГО МАТЕРИАЛА И ЯДЕРНЫХ УСТАНОВОК (ПРАКТИЧЕСКОЕ ПРИМЕНЕНИЕ РЕКОМЕНДАЦИЙ INFCIRC/225/REVISION 5)

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
ГАНА
ГВАТЕМАЛА
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
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
НИДЕРЛАНДЫ
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, № 27-G

ФИЗИЧЕСКАЯ ЗАЩИТА ЯДЕРНОГО МАТЕРИАЛА И ЯДЕРНЫХ УСТАНОВОК (ПРАКТИЧЕСКОЕ ПРИМЕНЕНИЕ РЕКОМЕНДАЦИЙ INFCIRC/225/REVISION 5)

ПРАКТИЧЕСКОЕ РУКОВОДСТВО

МЕЖДУНАРОДНОЕ АГЕНТСТВО ПО АТОМНОЙ ЭНЕРГИИ
ВЕНА, 2022 ГОД

УВЕДОМЛЕНИЕ ОБ АВТОРСКОМ ПРАВЕ

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

Группа маркетинга и сбыта (Marketing and Sales Unit)
Издательская секция
Международное агентство по атомной энергии
Венский международный центр,
а/я 100,
A1400 Вена, Австрия
Факс: +43 1 26007 22529
Тел.: +43 1 2600 22417
Эл. почта: sales.publications@iaea.org
https://www.iaea.org/ru/publikacii

© МАГАТЭ, 2022

Отпечатано МАГАТЭ в Австрии,
октябрь 2022 года
STI/PUB/1760

ФИЗИЧЕСКАЯ ЗАЩИТА ЯДЕРНОГО
МАТЕРИАЛА И ЯДЕРНЫХ УСТАНОВОК
(ПРАКТИЧЕСКОЕ ПРИМЕНЕНИЕ РЕКОМЕНДАЦИЙ
INFCIRC/225/REVISION 5)
МАГАТЭ, ВЕНА, 2022 ГОД
STI/PUB/1760
ISBN 978–92–0–424721–3 (печатный формат)
ISBN 978–92–0–424821–0 (формат pdf)
ISSN 2788–8959

ПРЕДИСЛОВИЕ

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

Обеспечение физической ядерной безопасности — долг каждого отдельно взятого государства, однако созданию и поддержанию эффективных режимов физической ядерной безопасности в немалой степени способствует международное сотрудничество. То, что МАГАТЭ играет центральную роль в содействии такому сотрудничеству и оказании помощи государствам, — общепризнанный факт. Эта роль обусловлена широким членским составом МАГАТЭ, его мандатом, уникальным экспертным потенциалом и давним опытом предоставления технической помощи и специальных практических руководящих материалов государствам.

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

Руководящие материалы разрабатываются при активном участии экспертов из государств — членов МАГАТЭ, благодаря чему в них находит отражение консенсус в отношении положительных практик в области физической ядерной безопасности. Комитет МАГАТЭ по руководящим материалам по физической ядерной безопасности, учрежденный в марте 2012 года и состоящий из представителей государств-членов, занимается рассмотрением и одобрением проектов публикаций Серии изданий по физической ядерной безопасности по мере их подготовки.

МАГАТЭ совместно с государствами-членами продолжит работать над тем, чтобы блага мирных ядерных технологий могли использоваться для улучшения здоровья, повышения уровня жизни и благосостояния людей.

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. Серия изданий МАГАТЭ по физической ядерной безопасности содержит руководства для государств с целью оказания им помощи в установлении и обеспечении устойчивости национального режима физической ядерной безопасности, а также в оценке и, при необходимости, укреплении этого режима. Данная серия также содержит руководства для государств по выполнению их обязательств по юридически обязательным международно-правовым документам и международным документам, не имеющим обязательной юридической силы.

1.2. Физическая защита ядерного материала и ядерных установок — важная часть режима физической ядерной безопасности государств, которые имеют такие материалы и установки. Документ № 13 Серии изданий МАГАТЭ по физической ядерной безопасности «Рекомендации по физической ядерной безопасности, касающиеся физической защиты ядерных материалов и ядерных установок» (INFCIRC/225/Revision 5) [1] был опубликован МАГАТЭ в 2012 году. Как явствует из названия, указанные рекомендации также являются 5-м пересмотренным изданием документа INFCIRC/225, руководством для государств по выполнению их обязательств в рамках Конвенции о физической защите ядерного материала и, после вступления в силу поправки к ней 2005 года, ее обновленной редакции.

1.3. Данная публикация — главное практическое руководство в комплекте руководящих документов для государств по применению «Рекомендаций» [1]. Несколько существующих практических руководств и технических руководящих материалов посвящены конкретным вопросам физической защиты ядерных материалов и ядерных установок, таким как проектная угроза, меры по противодействию инсайдерским угрозам, культура физической ядерной безопасности и определение особо важных зон. Данное практическое руководство знакомит читателя с некоторыми из этих основных аспектов, содержит обзор их роли в физической защите и, при необходимости, ссылки на тематические руководства, которые содержат более конкретные рекомендации.

ЦЕЛЬ

1.4. Цель настоящей публикации — сформулировать руководящие указания и предложения для государств и их компетентных органов, призванные помочь им в установлении, укреплении и обеспечении устойчивости национальных режимов физической защиты, а также применении сопутствующих систем и мер, в том числе систем физической защиты оператора. В некоторых частях настоящей публикации намеренно не дается конкретных указаний по распределению ответственности между государством и его компетентными органами ввиду различий, существующих между государствами в этой связи. Государствам следует тщательно и в полной мере распределить обязанности в области физической защиты между компетентными органами и отразить это в соответствующих документах.

ОБЛАСТЬ ПРИМЕНЕНИЯ

1.5. Настоящее практическое руководство применяется к физической защите ядерных установок и ядерного материала при их использовании и хранении от:

a) несанкционированного изъятия ядерных материалов с целью изготовления ядерного взрывного устройства;
b) саботажа (диверсии) в отношении ядерных материалов и ядерных установок, ведущего к радиологическим последствиям.

Настоящее практическое руководство также содержит некоторые предложения в отношении сопутствующих мер, которые могут способствовать координированному реагированию в части определения места нахождения и возвращения пропавшего ядерного материала и смягчения или сведения к минимуму радиологических последствий саботажа (диверсии на ядерных установках.

1.6. В настоящей публикации не содержится подробных руководящих указаний по следующим вопросам:

a) физическая защита ядерных материалов при их перевозке за пределами ядерной установки (такой защите посвящено специальное руководство [2]);

b) защита от несанкционированного изъятия ядерного материала с целью возможного последующего рассеяния за пределами площадки (такой защите посвящено руководство по физической безопасности радиоактивных материалов [3]).

Настоящее практическое руководство не содержит подробных рекомендаций по учету соображений физической ядерной безопасности при выборе площадки для установки и проектировании установок. Интеграция принципов физической защиты на как можно более ранних этапах жизненного цикла установки обычно называется «учетом требований безопасности при проектировании».

1.7. Государства могут решить установить требования по защите ядерного материала и ядерных установок на своей территории по ряду других причин, таких как экономическая значимость этих объектов, репутационные вопросы или потенциальные последствия прекращения производства атомной энергии. В настоящей публикации не содержится рекомендаций по решению этих дополнительных вопросов.

СТРУКТУРА

1.8. Структура настоящего практического руководства в целом, хотя и не во всех отношениях, повторяет структуру исходной публикации «Рекомендации» [1]:

a) вопросы физической защиты ядерного материала при его перевозке за пределами ядерной установки выходят за рамки данного практического руководства;
b) в данном руководстве в едином разделе излагается комплексный риск-ориентированный подход к обеспечению защиты от несанкционированного изъятия ядерного материала и саботажа (диверсии). В «Рекомендациях» [1] эти два аспекта рассматриваются в двух разных разделах.

1.9. Настоящая публикация построена следующим образом. В следующем за введении разделе 2 описываются цели физической защиты и общий подход к управлению рисками несанкционированного изъятия ядерного материала и саботажа (диверсии) в отношении ядерных установок. В разделе 3 государствам и их компетентным органам даются руководящие указания по элементам физической защиты в рамках режима физической

ядерной безопасности; данные указания базируются на основополагающих принципах, изложенных в «Рекомендациях» [1]. В разделе 4 даются руководящие указания по системе физической защиты оператора и описан системный, интегрированный подход. Приложение I представляет собой аннотированный набросок типового содержания плана обеспечения физической безопасности оператора. В приложении II даются аналогичные указания по плану чрезвычайных мер. В приложении III описан процесс агрегирования ядерного материала, который может быть использован для классификации ядерного материала и определения надлежащего уровня защиты от несанкционированного изъятия. Приложение IV представляет собой таблицу перекрестных ссылок между пунктами «Рекомендаций» [1] и настоящего практического руководства.

2. ЦЕЛИ ГОСУДАРСТВЕННОГО РЕЖИМА ФИЗИЧЕСКОЙ ЗАЩИТЫ

2.1. Четыре цели государственного режима физической защиты[1], описанные в [1], также изложены в поправке к Конвенции о физической защите ядерного материала и «Целях и основополагающих принципах физической зашиты», принятых Советом управляющих МАГАТЭ и Генеральной конференцией в 2001 году.

[1] Ранее для выражения концепции, которая теперь именуется «физической ядерной безопасностью ядерных материалов и ядерных установок», использовался термин «физическая защита», и в публикации [1] (которая является также 5-м пересмотренным изданием документа INFCIRC/225) используется термин «физическая защита» (включая использование термина «режим физической защиты» для аспектов режима физической ядерной безопасности, касающихся несанкционированного изъятия ядерного материала или саботажа (диверсии) в отношении ядерных материалов или ядерных установок). С целью содействия признанию настоящей публикации как руководства по практическому применению рекомендаций INFCIRC/225/Revision 5 термин «физическая защита» используется здесь применительно к тем аспектам физической ядерной безопасности, которые касаются несанкционированного изъятия ядерного материала или саботажа (диверсии) в отношении ядерных материалов или ядерных установок. Таким образом, например, государственный режим физической защиты включает те части режима физической ядерной безопасности, которые связаны с такими мерами.

«2.1. Общая цель государственного режима физической ядерной безопасности — это защита лиц, имущества, общества (людей) и окружающей среды от *злоумышленных действий*, связанных с *ядерными материалами* и другими радиоактивными материалами. Цели государственного *режима физической защиты*, который является важнейшим компонентом государственного режима физической ядерной безопасности, должны состоять в том, чтобы:

— **обеспечивать защиту от *несанкционированного изъятия***. — Защита от хищения или иного незаконного захвата *ядерного материала*;
— **определять место нахождения и обеспечивать возвращение пропавших *ядерных материалов*.** — Обеспечение осуществления оперативных и комплексных мер по обнаружению и в надлежащих случаях возвращению пропавших или похищенных *ядерных материалов*;
— **обеспечивать защиту от *саботажа (диверсии)*.** — Защита *ядерного материала* и *ядерных установок* от *саботажа (диверсии)*;
— **смягчать или сводить к минимуму последствия *саботажа (диверсии)***. — Смягчение или сведение к минимуму радиологических последствий *саботажа (диверсии)*.

«2.2. Следует добиваться, чтобы государственный *режим физической защиты* обеспечивал достижение этих целей путем:

— предупреждения *злоумышленных действий* посредством сдерживания и защиты чувствительной информации;
— пресечения попыток *злоумышленных действий* или *злоумышленных действий* посредством интегрированной системы *обнаружения*, задержки проникновения (продвижения) и реагирования;
— смягчения последствий *злоумышленного действия*.

2.3. Следует обеспечивать, чтобы достижение указанных выше целей осуществлялось интегрированным и координированным образом, с учетом различных рисков, которым противодействуют меры по обеспечению физической ядерной безопасности» [1].

2.2. С точки зрения физической ядерной безопасности двумя основными рисками, связанными с использованием ядерных материалов и ядерных установок, являются несанкционированное изъятие ядерного материала для потенциального применения в ядерном взрывном устройстве и саботаж

(диверсия) в отношении материала и/или установки с неприемлемыми радиологическими последствиями. Управление указанными рисками является первоосновой физической ядерной безопасности применительно к ядерным материалам и ядерным установкам. Если государство решает разместить ядерные материалы и ядерные установки на своей территории, то оно также принимает на себя ответственность за защиту этих материалов от несанкционированного изъятия и за защиту этих установок и материалов от саботажа (диверсии), который приводит к выбросу радионуклидов.

2.3. В публикации [1] государствам рекомендуется выработать подход к управлению рисками для достижения вышеуказанных целей, связанных с защитой от несанкционированного изъятия и саботажа (диверсии). Такой подход должен охватывать три аспекта, характеризующих риск: угрозу, потенциальные последствия и уязвимость. В [1] содержатся рекомендации, касающиеся:

a) оценки угроз и проектной угрозы;
b) потенциальных последствий несанкционированного изъятия ядерного материала (определенных с помощью таблицы категорирования ядерного материала) и саботажа (диверсии) (определенных на основе подхода к дифференциации радиологических последствий), что способствует применению дифференцированного подхода и принятию соразмерных мер физической защиты;
c) учета, при помощи эффективной системы физической защиты, уязвимостей целей внутри ядерной установки, которые в противном случае могут быть использованы нарушителем для успешного совершения злоумышленных действий.

2.4. Следует обеспечивать, чтобы государства, применяя «Рекомендации» [1], были способны надлежащим образом управлять риском злоумышленных действий, направленных на ядерные материалы или ядерные установки. Однако для надлежащего управления таким риском государства должны установить собственные детально разработанные цели физической ядерной безопасности, приняв во внимание дифференцированный подход.

2.5. С целью снижения риска оператор ядерной установки может заменить ядерный материал, являющийся более привлекательным для нарушителей, на ядерный материал, менее привлекательный для нарушителей, спроектировать установку с возможностью использования такого материала и/или с такими характеристиками, которые привели бы к менее тяжелым

радиологическим последствиям в случае саботажа (диверсии), и/или создать более надежные системы физической защиты. Кроме того, компетентные органы, занимающиеся разведывательной деятельностью и отвечающие за физическую ядерную безопасность, могут тесно взаимодействовать в деле обнаружения и пресечения планируемых нарушителем злоумышленных действий до того, как такие планы будут реализованы на ядерной установке. Реализация всех основополагающих принципов в рамках государственного режима физической ядерной безопасности и применение надлежащих мер физической защиты на ядерных установках имеют перед собой общую цель — защитить ядерные установки от злоумышленных действий.

3. ЭЛЕМЕНТЫ ГОСУДАРСТВЕННОГО РЕЖИМА ФИЗИЧЕСКОЙ ЯДЕРНОЙ БЕЗОПАСНОСТИ ДЛЯ ОБЕСПЕЧЕНИЯ ФИЗИЧЕСКОЙ ЗАЩИТЫ ЯДЕРНЫХ МАТЕРИАЛОВ И ЯДЕРНЫХ УСТАНОВОК

3.1. В публикации [1] режим физической защиты определяется как:

«Режим государства, включающий:

— законодательную и регулирующие основы, регламентирующие обеспечение физической защиты *ядерных материалов* и *ядерных установок*;
— учреждения и организации в государстве, ответственные за обеспечение реализации законодательной и регулирующей основы;
— системы *физической защиты* для установок и перевозки».

3.2. Государственным режимом физической ядерной безопасности также должно обеспечиваться надлежащее управление взаимодействием между физической защитой и учетом и контролем ядерного материала и между физической защитой и ядерной безопасностью. Долг государства — обеспечить, чтобы требования к учету и контролю ядерного материала, физической защите и ядерной безопасности не противоречили друг другу, а также чтобы указанные элементы по мере возможности подкрепляли друг друга.

3.3. В настоящем разделе:

a) перечислены основополагающие принципы и другие основные элементы государственного режима физической ядерной безопасности, касающиеся физической защиты ядерных материалов при их использовании и хранении и ядерных установок, как описано в [1, 4];
b) даются руководящие указания по применению государством каждого принципа в контексте физической защиты ядерных материалов и ядерных установок.

3.4. Для достижения целей государственного режима физической ядерной безопасности ядерных материалов и ядерных установок государству следует разработать требования по установлению, применению, поддержанию и обеспечению устойчивости своего режима физической защиты. В публикации [1] обязательствам государства в этой связи посвящены три отдельных раздела (3, 4 и 5), но в настоящем разделе эти практические указания сведены воедино.

ОТВЕТСТВЕННОСТЬ ГОСУДАРСТВА

«Ответственность за создание, введение и поддержание *режима физической защиты* внутри государства целиком возлагается на это государство. (ОСНОВОПОЛАГАЮЩИЙ ПРИНЦИП A: Ответственность государства)

3.1.Государственный *режим физической защиты* предназначается для всех *ядерных материалов* при их использовании, хранении и *перевозке (транспортировке)*, а также для всех *ядерных установок*. Государству следует обеспечивать защиту *ядерных материалов* и *ядерных установок* от *несанкционированного изъятия* и от *саботажа (диверсии)*» [1].

3.5. Государство выполняет свое обязательство путем создания законодательной и регулирующей основы, делегирования полномочий по регулированию одному или нескольким компетентным органам и возложения главной ответственности за создание систем физической защиты на операторов ядерных установок.

3.6. Всеобъемлющий режим физической ядерной безопасности ядерных материалов распространяется не только на их использование и хранение (в том числе на ядерных установках), но и на их физическую защиту при

перевозке. Государству следует обеспечивать также создание, применение и поддержание комплексной системы физической защиты при перевозке. Такая система должна применяться к перемещениям ядерного материала категорий I и II между двумя защищенными зонами на площадке. Оператор ядерной установки как отправитель или получатель ядерного материала также может быть наделен определенными обязательствами по обеспечению физической защиты радиоактивного материала, который ввозится на площадку или вывозится с нее. Дополнительные руководящие указания содержатся в [2].

3.7. Пункт 3.2 публикации [1] гласит:

> «Государственный *режим физической защиты* следует регулярно рассматривать и модернизировать, с тем чтобы он отражал изменения, происходящие в отношении *угроз*, и достижения в подходах к обеспечению физической защиты, в области систем и технологий, а также применение новых типов *ядерных материалов* и *ядерных установок*».

Одной из возможных причин пересмотра и модернизации режима физической защиты может быть решение о строительстве атомной электростанции в государстве, единственной ядерной установкой в котором является исследовательский реактор, содержащий только ядерный материал категории III. Более высокий уровень физической защиты, который необходим для атомной электростанции, потребует пересмотра существующего режима. Другим примером может служить изменение угрозы, о чем говорится в пунктах 3.55–3.63.

РАСПРЕДЕЛЕНИЕ ОТВЕТСТВЕННОСТИ ЗА ОБЕСПЕЧЕНИЕ ФИЗИЧЕСКОЙ ЗАЩИТЫ

> «3.8. Государству следует четко определять и распределять ответственность за обеспечение физической защиты между всеми уровнями соответствующих правительственных органов, включая силы реагирования, а также *операторами* и в надлежащих случаях перевозчиками. Следует обеспечивать надлежащую интеграцию и координацию ответственности в рамках государственного *режима физической защиты*. Следует устанавливать и фиксировать четкие

сферы разделения ответственности между соответствующими органами, в особенности в тех случаях, когда организация, ответственная за вооруженное реагирование, отделена от *оператора*» [1].

3.8. Государству следует наделить ответственностью за решение вопросов физической защиты надлежащие компетентные органы и другие государственные учреждения как минимум в отношении следующего:

a) разработка и актуализация проектной угрозы и/или оценки угроз;
b) лицензирование/выдача разрешений на ядерные установки и ядерные материалы при их использовании и хранении;
c) инспектирование и оценка систем физической защиты;
d) реагирование на события, связанные с физической ядерной безопасностью, включая действия сил реагирования и организаций аварийного реагирования;
e) управление взаимодействием с системой учета и контроля ядерных материалов;
f) управление взаимодействием с ядерной безопасностью;
g) управление информационной и компьютерной безопасностью, касающейся физической защиты ядерных установок и ядерных материалов при их использовании и хранении;
h) проверка благонадежности персонала;
i) меры борьбы с несоблюдением требований лицензий и правил физической защиты.

3.9. Государство может рассмотреть возможность учреждения надлежащих механизмов координации действий с целью выполнения этих обязанностей, таких как комитет государственных органов, ведающих вопросами физической защиты, который проводит регулярные совещания для укрепления коммуникации, взаимодействия и координации.

3.10. В рамках выполнения государством его обязательств в области физической защиты следует четко прописать обязанности соответствующих компетентных органов, которые обеспечивают реагирование на события, связанные с физической ядерной безопасностью, на ядерных установках. Следует развивать координацию между охраной, силами реагирования и соответствующими компетентными органами, и, в частности, следует регулярно отрабатывать совместные действия сил охраны и реагирования.

3.11. Каждое государство определяет свои собственные цели реагирования и может применять разные подходы или стратегии для использования сил реагирования. Указанные определения, подходы и стратегии могут зависеть от типа ядерных материалов и ядерных установок, которые ставятся под защиту, и от потенциальных намерений нарушителей (например, хищение, саботаж (диверсия)). На ядерных установках со значимыми целями для хищения и/или саботажа (диверсии) применяются следующие стратегии реагирования:

a) пресечение доступа, целью которого является предотвращение силами реагирования доступа нарушителя к цели;
b) недопущение выполнения задачи, целью которого является пресечение силами реагирования действий нарушителей (в том числе вовлеченных в эти действия внутренних нарушителей) до того, как они смогут успешно выполнить свою задачу;
c) сдерживание, целью которого является недопущение силами реагирования перемещения нарушителями материала за определенную черту, такую как граница зоны ограниченного доступа, чтобы тем самым не допустить утраты регулирующего контроля над ним.

ЗАКОНОДАТЕЛЬНАЯ И РЕГУЛИРУЮЩАЯ ОСНОВА

«Государство несет ответственность за создание и поддержание законодательной и регулирующей основы для регулирования физической защиты. Эта основа должна обеспечивать установление применимых требований физической защиты и включать систему оценки и лицензирования или другие процедуры для выдачи разрешений. Эта основа должна включать систему инспектирования *ядерных установок* и *транспортных средств* для проверки соблюдения применимых требований и условий лицензии или другого санкционирующего (разрешительного) документа, а также установить механизм обеспечения соблюдения применимых требований и условий, в том числе эффективные санкции. (ОСНОВОПОЛАГАЮЩИЙ ПРИНЦИП С: Законодательная и регулирующая основа)

3.9. Государству следует принимать соответствующие меры в рамках своего национального законодательства с целью создания и обеспечения надлежащего введения в действие и функционирования государственного *режима физической защиты*» [1].

Подходы к регулированию

3.12. Государствам следует разработать и ввести в действие регулирующие положения, соответствующие законодательной основе государства. Точный характер и содержание регулирующих положений будет зависеть от решений, принятых государством в отношении порядка выполнения регулирующих функций, включая количество компетентных органов, занятых надзором за режимом физической защиты.

3.13. Государство несет ответственность за проведение оценки угроз, и уполномоченному компетентному органу может быть поручена разработка проектной угрозы, которая при необходимости будет вестись в консультации с другими соответствующими государственными органами. В любом случае компетентный орган использует информацию об угрозах как основу для разработки общих требований и целевых значений, а также критериев оценки соответствия или эффективности. Применяя дифференцированный подход, компетентный орган определяет цели физической защиты и/или требования по защите каждой категории ядерного материала и по предотвращению каждого уровня потенциальных радиологических последствий (на уровне или выше предела неприемлемых радиологических последствий) на ядерных установках.

3.14. Государству следует обеспечить, чтобы режим физической ядерной безопасности был и оставался основанным на актуальном анализе угроз, поскольку физическая защита ядерного материала и ядерных установок должна быть эффективна против угроз. Существуют три разных подхода к установлению требований в рамках регулирующей основы для устранения угрозы. Это следующие подходы: подход, ориентированный на достижение определенных показателей, предписывающий подход и подход, совмещающий в себе элементы двух указанных подходов. В зависимости от ситуации может быть использован один из двух подходов либо их сочетание, но рекомендации в [1], касающиеся оценки и проверки функционирования, в основном имеют отношение к подходу, ориентированному на достижение определенных показателей, который используется сам по себе или в сочетании с предписывающим подходом.

3.15. Подход, ориентированный на достижение определенных показателей — это в большей степени количественный подход к обеспечению и проверке эффективности физической защиты, и он может быть особенно полезен при защите ядерного материала с более высоким риском несанкционированного изъятия, а также защите ядерных материалов

и ядерных установок от саботажа (диверсии). Это необязательно означает, что предписывающий подход сам по себе не подходит для таких случаев, однако предписывающие требования часто проще применять для проверки того, принимаются ли отдельные меры физической защиты, чем для демонстрации систематической эффективности посредством проверки функционирования. Какой бы подход ни использовался, требования или цели должны быть оговорены, а эффективность соответствующих мер должна проверяться компетентным органом.

3.16. Регулирующие требования, установленные компетентным органом, должны быть направлены на устранение угрозы, определенной в ходе оценки угроз или в проектной угрозе. Проектная угроза служит основой для создания системы физической защиты. Система физической защиты ядерной установки должна быть спроектирована оператором в соответствии с применимыми регулирующими требованиями и одобрена компетентным органом.

3.17. Проверка функционирования отдельных мер физической защиты и системы физической защиты рекомендована в [1] для ядерных установок, на которых имеются ядерные материалы категории I и категории II, и ядерных установок, включая атомные электростанции, саботаж (диверсия) в отношении которых может привести к тяжелым радиологическим последствиям.

Подход, ориентированный на достижение определенных показателей

3.18. При подходе, ориентированном на достижение определенных показателей, государство определяет цели физической защиты на основе оценки угроз и, если применимо, проектной угрозы с учетом дифференцированного подхода. Государство обязывает оператора проектировать и создавать систему физической защиты, которая соответствовала бы этим целям, достигая определенного уровня эффективности в обеспечении защиты от злоумышленных действий и предусматривая реагирование в чрезвычайных ситуациях.

3.19. Подход, ориентированный на достижение определенных показателей, дает возможность оператору предложить комбинацию мер физической защиты, подходящую для конкретной установки. Например, оператор может создать систему физической защиты, которая позволяет задержать нарушителя лишь на короткое время, но это компенсируется быстрым и эффективным реагированием. Достаточность таких мер сравнивается с

результатами оценки угроз или проектной угрозой, чтобы удостовериться в том, что комплекс мер, основанных на достижении определенных показателей, соответствует целям системы физической защиты.

3.20. Преимуществом подхода, ориентированного на достижение определенных показателей, является его исходная посылка, что эффективность системы физической защиты может быть достигнута множеством комбинаций мер физической защиты и что каждая установка и ее эксплуатационные условия могут быть разными. При использовании подхода, ориентированного на достижение определенных показателей, следует определить возможные варианты создания такой системы физической защиты, которая отвечала бы целям и требованиям физической защиты, а также учитывала специфику данной площадки.

3.21. Реализация подхода, ориентированного на достижение определенных показателей, зависит от наличия как у компетентного органа, так и у оператора достаточных экспертных знаний в области физической безопасности соответственно для того, чтобы устанавливать требования и создавать системы на основе оценки физической защиты. Подход, ориентированный на достижение определенных показателей, также обязательно предполагает предоставление государством оператору чувствительной информации об оценке угроз или проектной угрозе, а оператор должен быть способен обеспечить надлежащую защиту такой чувствительной информации.

Предписывающий подход

3.22. В рамках предписывающего подхода государство определяет конкретные меры физической защиты, которые оно считает нужными для достижения поставленных им целей физической защиты по каждой категории ядерного материала и каждому уровню потенциальных радиологических последствий. Результатом является минимальный набор мер для реализации оператором.

3.23. Преимуществами предписывающего подходя являются простота его применения государством и оператором, отсутствие необходимости передачи государством оператору чувствительной информации в форме оценки угроз или проектной угрозы, а также простота инспектирования и оценки. Использование предписывающего подхода может быть особенно уместным в тех случаях, когда и уровень угрозы, и уровень потенциальных последствий являются низкими. Примером служат ядерные материалы

категории III, которые хранятся или используются в условиях относительно низкого уровня угрозы. Предписывающий подход также более уместен в тех случаях, когда проведение детальной оценки угроз или разработка проектной угрозы нецелесообразны.

3.24. Предписывающий подход может быть недостаточно гибким в конкретных обстоятельствах. Кроме того, при данном подходе оператор не обязан обеспечивать, чтобы применяемые меры физической безопасности были достаточными: основная ответственность за устранение риска лежит на государстве, поскольку именно государство точно указывает, какие меры физической защиты необходимы для устранения угрозы. Оператор отвечает только за эффективность отдельных мер физической защиты во время эксплуатации и поддержания работоспособности системы физической защиты.

Комбинированный подход

3.25. Комбинированный подход включает в себя элементы как предписывающего подхода, так и подхода, ориентированного на достижение определенных показателей. Существует множество путей применения комбинированного подхода, два из которых состоят в следующем:

a) государство может требовать применения подхода, ориентированного на достижение определенных показателей, для ядерных материалов, злоумышленное использование которых может иметь наиболее серьезные последствия, и разрешить применение предписывающего подхода для ядерных материалов, потенциальные последствия от злоумышленного использования которых относительно менее серьезны;
b) государство может требовать соблюдения некоего набора предписывающих требований в отношении конкретно оговоренных аспектов физической безопасности (например, защита чувствительной информации, проверка благонадежности персонала); данные требования будут дополнять собой меры в отношении всех других аспектов, которые будут вырабатываться на основе подхода, ориентированного на достижение определенных показателей.

3.26. Основным преимуществом комбинированного подхода является его гибкость. Ограничения комбинированного подхода схожи с ограничениями предписывающего подхода и подхода, ориентированного на достижение

определенных показателей, и будут зависеть от конкретного способа реализации подхода, выбранного государством. Тем не менее грамотно примененный комбинированный подход может обеспечить надлежащий баланс и уменьшить влияние ограничений, присущих каждому из указанных подходов.

Оценка системы физической защиты, включая проверку функционирования: требования государства

3.27. В рекомендациях, сформулированных в [1], делается акцент на важности оценки систем физической защиты, включая проверку функционирования. Например:

a) законодательная и регулирующая основа должна «**обеспечивать установление применимых требований физической защиты и включать систему оценки**» ([1], основополагающий принцип C);
b) законодательная и регулирующая основа должна «обеспечивать, чтобы оценки включали мероприятия по проверке *системы физической защиты*, включая уровень подготовки и оперативную готовность *сотрудников охраны* и/или *сил реагирования*» ([1], пункт 3.13);
c) компетентному органу следует «обеспечивать, чтобы проводились оценки, основанные на *проверке функционирования*, *операторами* на *ядерных установках*» ([1], пункт 3.21);
d) в программы обеспечения устойчивости «следует включать: ... *проверку функционирования* и оперативный мониторинг» ([1], пункт 3.57).

3.28. Все операторы ядерных установок должны проводить оценку системы физической защиты своих установок, включая проверку функционирования; в этих оценках должны учитываться система учета и контроля ядерных материалов, вопросы информационной безопасности и компьютерной безопасности.

3.29. Оценка систем физической защиты обычно состоит из проверки и анализа. Проверка может проводиться на уровне отдельных компонентов, подсистем и систем и может охватывать аппаратные средства/оборудование, программное обеспечение, людей и процедуры. Анализ может включать качественные и/или количественные методы и предполагать использование моделирования и имитации. Методы моделирования и имитации могут включать создаваемые вручную или при помощи компьютера математические модели, компьютерное моделирование боевых действий,

кабинетные учения, ограниченные и полномасштабные учения сил реагирования и двухсторонние учения. Оценка систем физической защиты должна всегда включать проведение определенных учений.

3.30. Разные методы потребуют разного объема данных (с разными требованиями к качеству), дадут разные типы информации, будут иметь разные ограничения и потребуют разного объема ресурсов. Используя дифференцированный подход, компетентный орган должен определить минимальный набор мер по оценке системы физической защиты, включая требования к проверке функционирования. Данные регулирующие требования могут касаться функций и обязанностей, требуемых и/или разрешенных методов, документации и периодичности оценки и проверки. Например, некоторые оценки и учения должны проводиться не реже одного раза в год; более комплексные учения (такие как двухсторонние учения) могут проводиться реже, но как минимум раз в два-три года.

3.31. Компетентному органу следует анализировать проведенную оценку системы физической защиты, включая проверку функционирования, например, путем подтверждения того, что использованные при оценке и проверке данные и методы корректны и что результаты оценки и проверки дают точную характеристику системе физической защиты.

3.32. Компетентный орган может рассмотреть возможность привлечения независимой третьей стороны с надлежащей компетенцией для проведения проверки функционирования. Одним из примеров будет проверка функции задержки на образцах заграждений с использованием средств нарушителя, определенных в ходе оценки угроз или в проектной угрозе.

Лицензирование и другие процедуры выдачи официальных разрешений

> «3.12. Государству следует осуществлять выдачу лицензии или официального разрешения на данную деятельность только в том случае, если она соответствует правилам физической защиты. Государству следует предусматривать проведение *компетентным органом* государства тщательного изучения предложенных *мер физической защиты* с целью их оценки, необходимой для утверждения этой деятельности до выдачи лицензии или официального разрешения, и в случае внесения значительных изменений для обеспечения постоянного соблюдения правил физической защиты» [1].

3.33. Главная ответственность за осуществление мер физической защиты ядерного материала лежит на каждом операторе, государственный контроль за обеспечением физической защиты осуществляется в основном путем выдачи лицензий (или официальных разрешений) правительством или регулирующим органом. Лицензия должна представлять собой официальный документ, дающий разрешение на эксплуатацию установки или осуществление деятельности (такой как ввоз ядерного материала на ядерную установку или вывоз с нее). Первоочередной задачей государства является установление лицензионных требований к системам физической защиты и решение вопроса об одобрении заявок на получение новых лицензий и возобновление или изменение существующих лицензий. План обеспечения физической безопасности оператора представляется заявителем в рамках процесса лицензирования оператора ядерной установки, и выполнение положений утвержденного плана обеспечения физической безопасности должно быть условием выдачи лицензии.

3.34. Лицензирование — это непрерывный процесс, охватывающий все стадии жизненного цикла ядерной установки. Лицензия может быть изменена, приостановлена или аннулирована — в зависимости от условий и работы оператора, — но делаться это может только государством и под контролем государства.

3.35. Государство должно выдавать лицензии на эксплуатацию установок и осуществление деятельности только при соблюдении ими требований государства в отношении физической защиты. Во всех выдаваемых лицензиях предлагается указывать:

a) наименование конкретной установки или вида деятельности, на которые выдается лицензия;
b) любые особые требования, условия, временные рамки и другие ограничения;
c) конкретный перечень обязанностей лицензиата.

3.36. До выдачи лицензии и ввоза ядерного материала на установку государству следует убедиться в том, что компетентный орган получил, оценил и одобрил план обеспечения физической безопасности заявителя или оператора в отношении установки или деятельности, на которые выдается лицензия. Эта оценка должна подкрепляться анализом системы физической защиты, предложенной для установки. Если будут выявлены какие-либо недостатки, государство может отложить выдачу лицензии до тех пор, пока указанные недостатки не будут устранены и система

физической защиты не будет признана соответствующей требованиям. В качестве альтернативы государство может утвердить лицензию с условием, что эти недостатки должны быть устранены в течение определенного срока.

3.37. Дополнительные руководящие указания по процессу лицензирования содержатся в [5].

Обеспечение выполнения регулирующих положений

3.38. Обеспечение выполнения регулирующих положений в области физической защиты, а также выполнения условий лицензии при помощи эффективной законодательной и регулирующей основы — необходимый элемент государственного режима физической защиты. Для защиты ядерных материалов и ядерных установок государство должно наделить соответствующий компетентный орган полномочиями для возбуждения судебных дел или применения санкций на основании закона. Такие санкции могут включать приостановление или аннулирование лицензии и/или другие формы наказания физических или юридических лиц.

Компетентный орган

> **«Государству следует учредить или назначить *компетентный орган*, который будет нести ответственность за реализацию законодательной и регулирующей основы и наделен соответствующими полномочиями, компетенцией, финансовыми и людскими ресурсами для выполнения порученных ему обязанностей. Государству следует предпринять шаги для обеспечения действенной независимости между функциями *компетентного органа* государства и функциями любого другого органа, занимающегося вопросами содействия применению или использования ядерной энергии. (ОСНОВОПОЛАГАЮЩИЙ ПРИНЦИП D: *Компетентный орган*)»** [1].

3.39. Действенная независимость означает возможность компетентного органа, отвечающего за физическую ядерную безопасность, обеспечивать выполнение требований и регулирующих положений, необходимых для физической ядерной безопасности, без вмешательства тех, кто занимается вопросами содействия применению или использования ядерной энергии или других ядерных применений. Функционирование, финансирование и укомплектование штатами компетентного органа должно осуществляться независимо от органов, связанных с содействием применению или

использованием ядерной энергии. Для осуществления своих функций и выполнения своих обязанностей соразмерно характеру и количеству ядерных установок и видов деятельности, подлежащих регулированию, компетентному органу необходимо иметь доступ к достаточным финансовым ресурсам и возможность нанимать достаточное число квалифицированных и компетентных сотрудников. Для надлежащего выполнения своих функций компетентному органу рекомендуется составить планы работы с людскими ресурсами, в которых будут определены необходимый уровень кадрового обеспечения и объем учебной работы.

Роль компетентного органа в установлении требований, касающихся плана обеспечения физической безопасности

> «3.27. ...*Компетентному органу* следует рассматривать и утверждать план обеспечения физической безопасности, осуществление которого должно затем стать частью условий лицензии» [1].

3.40. Компетентному органу следует подробно разъяснять заявителям на получение лицензии и операторам те требования, которые они должны соблюдать при проектировании и создании системы физической защиты, которая будет приемлема для компетентного органа в соответствии с законодательной и регулирующей основой государства в области физической защиты. Важным элементом является разработка и выполнение оператором плана обеспечения физической безопасности, соответствующего категории ядерных материалов, находящихся под защитой, и уровню потенциальных радиологических последствий саботажа (диверсии). Компетентному органу рекомендуется разработать инструкции для операторов по требованиям, предъявляемым к плану обеспечения физической безопасности, с тем чтобы в нем были учтены все элементы государственных требований по обеспечению физической защиты.

3.41. План обеспечения физической безопасности является основным документом, описывающим систему физической защиты, который призван удовлетворить требования, установленные компетентным органом. Государству следует указать, какая информация в плане обеспечения физической безопасности нуждается в защите как чувствительная и как следует обеспечить такую защиту. Аннотированный предлагаемый набросок комплексного плана обеспечения физической безопасности содержится в приложении I.

Роль компетентного органа в составлении программы инспектирования

> «3.20. На *компетентный орган* государства следует возлагать ответственность за проверку постоянного соблюдения правил физической защиты и определенных лицензиями условий путем проведения регулярных инспекций и за обеспечение принятия при необходимости корректирующих мер» [1].

3.42. Цель программы инспектирования — удостовериться в том, что меры физической защиты действительно введены и соответствуют регулирующим требованиями и применимым условиям лицензии. Данный процесс должен включать подтверждение того, что утвержденный план обеспечения физической безопасности эффективно реализуется. В случае невыполнения регулирующих требований или условий лицензии следует рассмотреть возможность принятия регулирующих и/или правоприменительных мер и могут быть применены соответствующие и соразмерные меры или санкции.

3.43. Компетентный орган должен обеспечить, чтобы его инспекторы имели необходимую квалификацию, подготовку и опыт для осуществления своих обязанностей. Компетентный орган может определить требования к квалификации и подготовке инспекторов.

3.44. Программа инспектирования должна включать инспекции с уведомлением и без уведомления, позволяющие удостовериться в том, что система мер, предусмотренных в утвержденном плане обеспечения физической безопасности, действует у оператора постоянно, а не только во время запланированной проверки. Инспекции могут проводиться в любой момент — в рабочее и нерабочее время — и затрагивать всю регламентную и нерегламентную эксплуатационную деятельность, которая осуществляется на ядерных установках на текущий момент (например, во время останова реактора для технического обслуживания и перегрузки топлива). Рекомендуется, чтобы программа инспектирования предусматривала оценку и проверку всех мер физической защиты, включая технические, процедурные и административные положения. Инспекции следует проводить таким образом, чтобы они не создавали излишних помех и трудностей для эксплуатации установки. Если инспекция выявит какие-либо недостатки в системе физической защиты, компетентному органу следует убедиться, что оператор принял компенсирующие меры для обеспечения надлежащего уровня защиты до тех пор, пока недостатки не будут устранены и не будет достигнута достаточная эффективность системы.

3.45. Если инспекторы выявят несоблюдение требований или другие проблемы, вызывающие обеспокоенность, последующие процедуры инспекции должны включать подтверждение того, что оператор принял все корректирующие меры. Рекомендуется, чтобы такие меры носили дифференцированный характер и принимались в соответствии с категорией ядерного материала, находящегося в наличии, и потенциальными последствиями саботажа (диверсии). Инспекторам будет необходимо проконтролировать прогресс и проверить последующие действия с целью убедиться в том, что принятые корректирующие меры отвечают приемлемому стандарту и что достигнут эффективный уровень защиты. Компетентному органу следует утвердить корректирующие меры, и они должны быть включены в обновленный план обеспечения физической безопасности. В некоторых случаях для возвращения к нормальным условиям эксплуатации после принятия корректирующих мер может требоваться только уведомление компетентного органа, а не получение ясно выраженного согласия от компетентного органа.

3.46. Количество инспекций, запланированных для конкретной установки, может быть определено компетентным органом на основе категории материала, находящегося под защитой, уровня потенциальных радиологических последствий саботажа (диверсии), оценки угроз или проектной угрозы и других соответствующих факторов. При определении частоты инспекций может быть также принята во внимание репутация оператора в плане соблюдения требований. Время от времени могут также требоваться внеплановые инспекции, например после события, связанного с физической ядерной безопасностью, на ядерной установке или изменения угрозы.

Своевременное извещение о событиях, связанных с физической ядерной безопасностью

> «3.22. В государственном *режиме физической защиты* следует предусматривать требования в отношении своевременного извещения или предоставления сведений о *событиях, связанных с физической ядерной безопасностью*, и соответствующей информации, с тем чтобы *компетентный орган* государства был информирован о любых изменениях на *ядерных установках* или при *перевозке (транспортировке) ядерного материала*, которые могут оказать воздействие на осуществление *мер физической защиты*» [1].

3.47. Государству следует определить типы событий, о которых оператор должен извещать компетентный орган, и приемлемые сроки, в течение которых должно делаться такое извещение. Компетентный орган должен получать своевременную информацию обо всех значительных событиях, которые связаны с несанкционированными действиями, влияющими на физическую защиту ядерного материала или ядерных установок, например:

a) попытка проникновения или фактическое проникновение на установку или в обозначенную зону;
b) попытка несанкционированного изъятия или фактическое несанкционированное изъятие, потеря или несанкционированное перемещение ядерного материала с участием внешних или внутренних нарушителей;
c) попытка саботажа (диверсии) или фактически совершенный саботаж (диверсия);
d) обнаружение запрещенных предметов;
e) отклонение от утвержденного плана обеспечения физической безопасности (например, обесточивание оборудования физической защиты или повреждение заграждений вследствие погодных условий);
f) события с участием лиц, о которых следует докладывать в соответствии с государственной политикой обеспечения благонадежности;
g) потеря или несанкционированное разглашение чувствительной информации;
h) нарушение или попытка нарушения нормального функционирования компьютерных систем, используемых для обеспечения физической защиты, ядерной безопасности или учета и контроля ядерного материала (дополнительные руководящие указания см. в [6]).

3.48. Компетентный орган может быть обязан информировать другие государственные органы и участвовать в координированном реагировании на события, связанные с физической ядерной безопасностью. Оператор или компетентный орган может быть обязан расследовать инцидент с целью предотвращения повторения таких событий и извлечения уроков. Также могут потребоваться правоприменительные меры.

Ответственность обладателей лицензий

> **«Следует четко определить обязанности по реализации различных элементов физической защиты в государстве. Государству следует обеспечить, чтобы основная ответственность за осуществление физической защиты *ядерного материала* и *ядерных установок***

была возложена на обладателей соответствующих лицензий или других разрешительных документов (например, на *операторов* или *грузоотправителей*). (ОСНОВОПОЛАГАЮЩИЙ ПРИНЦИП Е: Ответственность обладателей лицензии)» [1].

3.49. Эта тема освещается в пунктах 4.4–4.13 об общих обязанностях оператора.

МЕЖДУНАРОДНОЕ СОТРУДНИЧЕСТВО И ПОМОЩЬ

3.50. Каждому государству следует рассмотреть вопрос о том, следует ли ему, и если да, то при каких условиях и в какой степени, сотрудничать с другими государствами, включая надлежащий обмен информацией и знаниями, полученными в рамках национального режима физической защиты. Такое решение должно приниматься с учетом необходимости защиты чувствительной информации о физической ядерной безопасности и соответствовать всем международным обязательствам и соглашениям об обмене информацией.

3.51. В [1] содержатся две рекомендации и одно предложение по международному сотрудничеству и помощи, касающиеся конкретно физической защиты ядерных установок, о чем подробнее говорится в следующих трех пунктах.

3.52. В [1], пункт 3.33, указывается следующее:

> «В случае *несанкционированного изъятия* или *саботажа (диверсии)*, или реальной угрозы этому государству следует в кратчайшие сроки предоставлять соответствующую информацию другим государствам, которых, по его мнению, это касается, а также информировать в надлежащих случаях Международное агентство по атомной энергии и другие соответствующие международные организации».

Информация может быть предоставлена в МАГАТЭ в добровольном порядке. В случае несанкционированного изъятия ядерного материала затронутому государству может оказаться особенно полезной помощь соседних государств в обнаружении и возвращении пропавших ядерных материалов, если такие материалы были ввезены в эти государства или проследовали транзитом через них. Обнаружение материала будет зависеть от систем(ы) обнаружения ядерного и другого радиоактивного материала,

находящегося вне регулирующего контроля, в государстве, в котором находится материал или границу которого он пересек. Дополнительные руководящие указания на этот счет содержатся в [7].

3.53. В [1], пункт 3.32, указывается: «Государствам следует информировать Международное агентство по атомной энергии и другие государства в соответствующем случае о надлежащих пунктах связи по вопросам, имеющим отношение к обеспечению физической защиты *ядерных материалов* и *ядерных установок*». В случае несанкционированного изъятия или саботажа (диверсии) пункты связи государств по вопросам физической защиты играют особенно важную роль с точки зрения более быстрой и точной передачи необходимых сведений соседним государствам и другим заинтересованным сторонам — напрямую или через МАГАТЭ[2]. Такие пункты связи могут также быть полезными при передаче другой важной информации, относящейся к физической защите, такой как информация о новых угрозах, общих для государств.

3.54. В [1], пункт 3.31, указывается: «Государствам рекомендуется сотрудничать и проводить консультации, а также обмениваться информацией по методам и практике обеспечения физической защиты непосредственно между собой либо через Международное агентство по атомной энергии и другие соответствующие международные организации». Государства, эксплуатирующие ядерные установки, имеют опыт и передовые наработки в области физической защиты и извлекли соответствующие уроки. Распространение такой информации среди государств может принести пользу мировому сообществу, содействуя росту общего уровня физической защиты ядерного материала. Несмотря на то что некоторую чувствительную информацию о конкретных установках распространять нельзя, множеством полезных сведений можно делиться на семинарах-практикумах, в рамках учебных программ и конференций. МАГАТЭ является полезным каналом для распространения такой информации без необходимости ссылки на источник.

---

[2] Что касается событий, связанных с физической ядерной безопасностью, в результате которых возникла ядерная или радиологическая аварийная ситуация, то предоставление информации о таком событии и оказание помощи должно осуществляться посредством оперативных механизмов, созданных МАГАТЭ в рамках Конвенции об оперативном оповещении и Конвенции о помощи и норм безопасности МАГАТЭ в области аварийной готовности и реагирования.

«Государственную систему физической защиты следует основывать на проводимой государством оценке угрозы. (ОСНОВОПОЛАГАЮЩИЙ ПРИНЦИП G: Угроза)

«3.34. На основании различных источников достоверной информации соответствующим государственным органам следует определять *угрозы* и соответствующий потенциал путем *оценки угроз* и, в надлежащих случаях, определения *проектной угрозы*. Определение *проектной угрозы* осуществляется на основе оценки государством угрозы *несанкционированного изъятия* и *саботажа (диверсии)»* [1].

3.55. Оценка угроз — это анализ существующих на настоящий момент угроз, в котором характеризуются мотивы, намерения и возможности потенциальных нарушителей для совершения злоумышленных действий. При оценка угроз учитываются угрозы терроризма и других противоправных и намеренных несанкционированных действий с ядерным материалом и ядерными установками или направленных против них, особенно несанкционированное изъятие ядерного материала и саботаж (диверсия) в отношении ядерного материала и ядерных установок. При оценке угроз также учитываются угрозы, исходящие как от внешних, так и от внутренних нарушителей. При проведении оценки угроз при необходимости используются внутренние, транснациональные и глобальные источники информации об угрозах.

3.56. Государства обладают разными возможностями для обнаружения и анализа угроз. Некоторые государства обладают широкими и многоплановыми возможностями в области безопасности и разведки, которые могут помочь государству в понимании природы и значительности угроз, в том числе тех, которым могут подвергаться ядерный материал и ядерные установки. В других случаях для обнаружения потенциальной угрозы внутри государства необходимо изучить и проанализировать общую информацию о национальной угрозе (например, районы гражданских беспорядков, преступная деятельность, присутствие террористов) и международных угрозах.

3.57. На компетентный орган следует возложить общую ответственность за проведение оценки угроз, которая потребует взаимодействия между всеми государственными учреждениями, несущими ответственность за анализ

угрозы и реагирование на нее (например, службы разведки, полиция, армия, таможенные и пограничные службы, местные правоприменительные органы). Поскольку такая работа потребует использования чувствительной информации, при оценке угроз и определении соответствующей проектной угрозы должны приниматься надлежащие меры по защите информации.

3.58. Дополнительные руководящие указания по оценке угроз и определению проектной угрозы на основе оценки угроз содержатся в [8]. В этом руководстве высказываются соображения по поводу использования проектной угрозы либо альтернативного заключения об угрозах. («Альтернативное заключение об угрозах», указанное в [8], представляет собой менее строгий подход к определению угрозы для проектирования систем физической защиты.)

3.59. Проектная угроза может использоваться компетентным органом по-разному. В рамках подхода, ориентированного на достижение определенных показателей, проектная угроза может использоваться оператором для проектирования системы физической защиты, а компетентным органом — для оценки системы физической защиты. В рамках предписывающего подхода для определения мер физической защиты, обязательных для применения оператором, компетентному органу может быть достаточно оценки угроз — за исключением случаев, когда речь идет о ядерном материале категории I и/или когда саботаж (диверсия) в отношении ядерной установки может потенциально привести к серьезным радиологическим последствиям. В последних случаях государственные требования к физической защите должны базироваться на проектной угрозе конкретно для несанкционированного изъятия ядерного материала категории I и саботажа (диверсии) в отношении ядерных материалов и ядерных установок.

3.60. В [1], пункт 3.36, указывается:

> «При рассмотрении угрозы должное внимание следует уделять *внутренним нарушителям*. Последние могут пользоваться своими правами доступа, а также имеющимися у них полномочиями и знаниями для обхода специальных элементов физической защиты или других предусмотренных мер, таких как процедуры обеспечения безопасности. Следует обеспечивать, чтобы *система физической защиты* поддерживалась мерами по учету и контролю ядерных

материалов с целью сдерживания и обнаружения хищения *ядерного материала внутренним нарушителем*, совершаемого на протяжении длительного времени».

МАГАТЭ опубликовало специальное руководство [9] для помощи государствам в устранении угроз, исходящих от внутренних нарушителей.

3.61. При оценке угроз и определении проектной угрозы следует учитывать возможные атаки на компьютерные системы, включая системы контроля и управления и другие системы, необходимые для ядерной безопасности, учета и контроля ядерного материала, а также систему физической защиты. Указанные системы включают в себя базы данных, систему контроля доступа и систему управления тревожной сигнализацией. При оценке угроз для перечисленных систем следует учитывать не только атаки, направленные на выведение из строя или уничтожение систем, но и менее прямые атаки, такие как подмена или фальсификация данных. Также следует учитывать потенциальные возможности нарушителей с точки зрения создания как внутренних, так и внешних угроз. В [6] содержатся дополнительные руководящие указания в отношении этого типа угроз.

3.62. Оценка угроз или проектная угроза должны учитывать возможные дистанционные нападения ([1], пункт 3.40), произведенные на расстоянии от ядерной установки. Указанные атаки не связаны с нарушителями, у которых есть доступ к цели или которым требуется преодолеть систему физической защиты. Примеры сценариев дистанционных нападений включают использование портативных ракетных пусковых установок или умышленное направление на ядерную установку воздушного судна. Государству следует определить, какие типы дистанционных нападений должны учитываться оператором.

3.63. Государству следует постоянно рассматривать угрозы и оценивать последствия любых изменений в оценке угроз или проектной угрозе. Например, государство может на ежегодной основе решать, требуется ли по результатам анализа угроз актуализация оценки угроз. События, связанные с физической ядерной безопасностью, внутри государства или где-либо еще могут стать причиной актуализации государством оценки угроз до намеченного периодического пересмотра. Государству следует постоянно проверять актуальность требований по обеспечению физической защиты в свете любых изменений в оценке угроз или проектной угрозе. В этом случае оператору потребуется проверить свою систему физической защиты

(включая проверку потенциальных целей для саботажа (диверсии)), и все последующие изменения в конструкции системы физической защиты до их внесения следует представить на утверждение в компетентный орган.

РИСК-ОРИЕНТИРОВАННЫЕ СИСТЕМЫ ФИЗИЧЕСКОЙ ЗАЩИТЫ

> «3.41. Государству следует посредством управления риском обеспечивать способность государственного *режима физической защиты* ограничивать и удерживать риски *несанкционированного изъятия* и *саботажа (диверсии)* на приемлемом уровне. Это требует оценки угрозы и потенциальных последствий *злоумышленных действий*, а затем разработки законодательной, регулирующей и программной основы, обеспечивающей применение надлежащих эффективных *мер физической защиты*» [1].

3.64. Оценка рисков в области физической ядерной безопасности включает в себя рассмотрение угроз, вероятности того, что злоумышленные действия могут быть успешно совершены источниками этих угроз, а также потенциальных последствий таких действий.

3.65. Государству следует использовать метод управления рисками с целью обеспечить, чтобы требования физической защиты и меры оператора по их выполнению позволяли удерживать риск, связанный с несанкционированным изъятием или саботажем (диверсией), на уровне, который государство считает приемлемым. Управление рисками предполагает периодический анализ угроз и потенциальных последствий злоумышленных действий и обеспечение наличия надлежащих систем физической защиты для предотвращения или достаточного уменьшения вероятности успешного совершения злоумышленных действий.

3.66. Управление рисками включает оценку риска, которая может быть количественной или качественной. Количественная оценка риска предполагает определение риска, связанного с конкретным событием, как выраженной в количественном отношении вероятности наступления события и ожидаемых последствий события в случае его наступления. Тем не менее расчет вероятности попытки совершить злоумышленное действие или успешности попытки очень сложен. Для целей планирования мер физической защиты может быть достаточно допустить, что попытка совершить злоумышленное действие будет непременно совершена. В этом случае указанный риск называется условным риском, где условием является

совершение попытки злоумышленного нападения. Условный риск может быть полезен для определения верхней границы количественной оценки риска и для сравнения рисков в случаях, в которых вероятность совершения попытки не является отличительным фактором (например, для сравнения разных вариантов обеспечения физической защиты против одного и того же риска).

3.67. В отсутствие количественных методов определения рисков в области физической ядерной безопасности для обоснования решений по обеспечению физической защиты могут быть использованы качественные подходы к управлению риском. Качественный подход к управлению риском означает рассмотрение вероятности попытки и успешности такой попытки без намерения рассчитать такую вероятность; вместо этого при качественном подходе к управлению риском принимается по внимание уязвимость цели(ей) перед угрозой и потенциальные последствия успешной реализации попытки. Данный подход может быть использован для определения комбинаций факторов, указывающих на высокий риск (например, высокая вероятность угрозы, большие потенциальные возможности нарушителя, серьезные последствия), и того, куда стоит направить усилия для более эффективного снижения риска. Аналогичным образом, комбинации факторов, указывающих на низкий риск, могут показывать, в каких случаях не требуются столь строгие меры физической безопасности.

3.68. Государство определяет критерии приемлемого функционирования системы физической защиты для противодействия несанкционированному изъятию обычно в привязке к проектной угрозе, потому что государство обязано принять на себя остаточный риск сбоя работы системы физической защиты. Государству также следует установить пределы неприемлемых радиологических последствий и серьезных радиологических последствий и взять их за основу для разработки требований к функционированию системы физической защиты для противодействия саботажу (диверсии). Если потенциальные радиологические последствия менее тяжелы, чем определенные государством неприемлемые радиологические последствия, следует обеспечить меры защиты оборудования и устройств, связанных с ядерной безопасностью, с помощью контроля доступа к ним и их охраны (подробнее об этом см. в пунктах 3.93–3.95). Практика управления риском позволяет обосновать надлежащее применение мер физической защиты при помощи дифференцированного подхода, о чем говорится ниже в пунктах 3.70–3.101.

3.69. При оценке рисков могут быть выявлены риски, требующие дополнительной оценки для определения того, необходимы ли дополнительные меры для их уменьшения. Риском можно управлять, например, посредством повышения эффективности сдерживания (например, повышение заметности принятых надежных мер физической защиты), усиления мер физической защиты (например, обеспечение дополнительной глубокоэшелонированной защиты) или уменьшения потенциальных последствий (например, изменение количества, типа, разбавления, химической или физической формы ядерного материала). Последствия таких изменений для ядерной безопасности также следует учитывать.

Дифференцированный подход

> **«Требования к физической защите следует основывать на *дифференцированном подходе*, учитывая результаты последней оценки угрозы, относительную привлекательность, характер *ядерного материала* и возможные последствия, связанные с *несанкционированным изъятием ядерного материала* и с *саботажем (диверсией)* в отношении *ядерного материала* или *ядерных установок*. (ОСНОВОПОЛАГАЮЩИЙ ПРИНЦИП Н: *Дифференцированный подход*)»** [1].

3.70. Государству следует основывать разработку требований и положений по обеспечению физической защиты на дифференцированном подходе, использующемся для обеспечения более высокого уровня защиты от событий, которые могут привести к более серьезным последствиям.

3.71. В целях градации мер защиты от несанкционированного изъятия ядерного материала для использования в ядерном взрывном устройстве категории ядерного материала, определенные в таблице 1 (основанной на публикации [1]), отражают относительную трудность использования данной категории материала для создания ядерного взрывного устройства. Ядерный материал категории I следует защищать самыми строгими мерами физической защиты; ядерный материал категории III необходимо защищать только исходя из соображений практической целесообразности ([1], пункт 4.12 и сноска с к таблице 1).

ТАБЛИЦА 1. КАТЕГОРИЗАЦИЯ ЯДЕРНОГО МАТЕРИАЛА *(основана на таблице 1 публикации [1])*

Материал	Форма	Категория I	Категория II	Категория III[c]
1. Плутоний[a]	Необлученный[b]	2 кг или более	Менее 2 кг, но более 500 г	500 г или менее, но более 15 г
2. Уран-235 (^{235}U)	Необлученный[b] – уран с обогащением по урану-235 от 20% или выше – уран с обогащением по урану-235 от 10%, но менее 20% – уран с обогащением по урану-235 выше природного, но менее 10%	5 кг или более	Менее 5 кг, но более 1 кг 10 кг или более	1 кг или менее, но более 15 г Менее 10 кг, но более 1 кг 10 кг или более
3. Уран-233 (^{233}U)	Необлученный[b]	2 кг или более	Менее 2 кг, но более 500 г	500 г или менее, но более 15 г
4. Облученное топливо (Приводимая в таблице категоризация облученного топлива основана на требованиях к международной перевозке. Государство, с учетом всех соответствующих факторов, может установить другую категорию для внутригосударственного использования, хранения и перевозки).			Обедненный или природный уран, торий или низкообогащенное топливо (с составом делящихся изотопов менее 10%)[d,e]	

ПРИМЕЧАНИЕ. Настоящая таблица не подлежит использованию или толкованию вне связи с текстом публикации [1].

[a] Весь плутоний за исключением плутония, изотопная концентрация которого превышает 80% по плутонию-238.

[b] Материал, не облученный в реакторе, или материал, облученный в реакторе, но с уровнем излучения, равным или менее 1 Гр/ч (100 рад/ч) на расстоянии 1 м без защиты (биологической).

[c] Защиту количества, не подпадающего под категорию III, а также природного урана, обедненного урана и тория следует обеспечивать как минимум исходя из соображений практической целесообразности.

[d] Хотя рекомендуется данный уровень защиты, государства могут, исходя из оценки конкретных обстоятельств, применить другую категорию физической защиты.

[e] Другое топливо, которое по своему первоначальному содержанию делящихся изотопов классифицируется по категории I или II до облучения, может быть понижено на одну категорию, если уровень излучения топлива превышает 1 Гр/ч (100 рад/ч) на расстоянии 1 м без защиты (биологической).

3.72. Для обеспечения защиты от саботажа (диверсии) государству следует учитывать потенциальные радиологические последствия таких действий и применять дифференцированный подход. Государству следует рассмотреть варианты защиты ядерных установок, принимая во внимание возможность возникновения неприемлемых радиологических последствий в результате саботажа (диверсии). Государству следует также обеспечить обязательное применение защитных мер в отношении тех целей на установке, которые могут привести к указанным последствиям при саботаже (диверсии).

3.73. Государству также следует рассмотреть возможность применения дифференцированного подхода при определении требований к другим мерам физической защиты, таким как обеспечение конфиденциальности чувствительной информации и проверка благонадежности физических лиц.

Градация уровней физической защиты исходя из последствий несанкционированного изъятия

Категоризация ядерного материала с точки зрения несанкционированного изъятия

> «4.5. Первичным фактором, рассматриваемым при определении мер физической защиты от *несанкционированного изъятия*, является сам *ядерный материал*. В таблице 1 различные типы *ядерного материала* разделены на категории с указанием элемента, изотопа, количества и степени облучения. Такая категоризация служит основой для применения *дифференцированного подхода* в обеспечении защиты от *несанкционированного изъятия ядерных материалов,* которые могут применяться в ядерном взрывном устройстве, что, в свою очередь, зависит от типа ядерного материала (например, плутоний и уран), изотопного состава (т.е. содержания делящихся изотопов), физической и химической формы, степени разбавления, уровня излучения и количества» [1].

3.74. В таблице 1, основанной на публикации [1], определены типы ядерного материала (например, плутоний или уран), уровни излучения, изотопный состав (т.е. содержание делящихся изотопов) и количества, которые устанавливают пределы для трех категорий (I–III) и косвенно для четвертой категории: «ниже категории III».

3.75. Для категоризации в таблице 1 используются четыре характеристики ядерного материала, указанные в [1], пункт 4.5: тип ядерного материала, изотопный состав, количество и облучение. В таблице 1 не указывается,

как использовать другие характеристики из этого пункта, такие как физическая и химическая форма и степень разбавления, как основу для дифференцированной защиты от несанкционированного изъятия ядерных материалов. Тем не менее в [1] указывается, что государство может принимать во внимание все эти характеристики.

Категоризация облученного топлива

3.76. В строке 4 таблицы 1 облученное топливо определено, по существу, как материал, облученный в реакторе с уровнем излучения не менее 1 Гр/ч (100 рад/ч) на расстоянии 1 м без защиты (биологической). В этой строке определено, что облученное топливо, которое до облучения состояло из обедненного или природного урана, тория или урана с обогащением по ^{235}U менее 10%, входит в категорию II несмотря на то, что ни одно из указанных видов топлива не попадает в категорию выше категории III до облучения. Причиной такой смены категории является то, что при облучении в реакторе в урановом топливе образуется плутоний (в основном ^{239}Pu), а в ториевом топливе аналогичным образом образуется ^{233}U. Процент плутония и ^{233}U, образующегося в результате облучения, относительно невелик (обычно около 1% от общей массы топлива в случае плутония). Однако в связи с тем, что такое облученное топливо обычно хранится в больших количествах, оно содержит достаточное количество ядерного материала (более 2 кг плутония или ^{233}U) для его отнесения к категории I. В соответствии с указанием в сноске е к таблице 1 категория такого облученного топлива может быть снижена на одну ступень (до категории II) из-за снижения его привлекательности ввиду его высокой радиоактивности.

3.77. В строке 4 таблицы 1 также указано, что по результатам оценки конкретных обстоятельств государство может предусмотреть другой уровень физической защиты вышеуказанных видов облученного топлива для их использования, хранения и перевозки внутри государства. Примером таких обстоятельств может быть место (такое как установка для послереакторных исследований), в котором хранится лишь небольшое количество облученных тепловыделяющих стержней. Из-за малого количества материала облученные тепловыделяющие стержни могут содержать менее 2 кг плутония или ^{233}U, и в таком случае будет достаточно обеспечить защиту облученного топлива как ядерного материала категории III. (Учетные документы для учета и контроля ядерного материала подтвердят, действительно ли речь идет о столь

малых количествах, поскольку в учетных документах должно указываться оценочное количество плутония или ^{233}U в облученном топливе, как и количество другого ядерного материала в этом топливе.)

3.78. В сноске е к таблице 1 указано, что другие виды топлива, относящиеся к категориям I и II до облучения, могут быть понижены на одну категорию после облучения. Данная сноска применима по указанным ниже причинам в следующих обстоятельствах.

a) Обычное топливо на основе плутония, смешанное оксидное топливо и топливо быстрых реакторов, как правило, содержит около 7% и 30% плутония соответственно. Несмотря на то что облучение в реакторе несколько снижает содержание плутония, оно не ведет к существенному уменьшению массовой концентрации плутония в облученном топливе. Поскольку такое топливо обычно хранится в больших объемах, количества плутония в облученном топливе в типичном хранилище будет достаточно для отнесения его к категории I. В соответствии со сноской е к таблице 1 категория такого топлива может быть понижена на одну ступень — до категории II — из-за высокого уровня его радиоактивности, снижающего его привлекательность.

b) Облучение в реакторе высокообогащенного уранового топлива (т.е. с обогащением по ^{235}U до 20% или выше) уменьшит содержание ^{235}U на несколько процентов. Тем не менее такое уменьшение обычно не сократит обогащение до уровня ниже 20%. Следовательно, облученное топливо будет и дальше состоять в основном из урана с обогащением 20% или выше. В итоге в соответствии со сноской е к таблице 1 находящееся в одном месте облученное высокообогащенное урановое топливо, общее содержание ^{235}U в котором до облучения составляет 5 кг или более, может быть перенесено из категории I в категорию II, а высокообогащенное урановое топливо с содержанием ^{235}U до облучения более 1 кг, но менее 5 кг может быть перенесено из категории II в категорию III. Такое снижение категории свидетельствует о том, что привлекательность материала уменьшается из-за высокого уровня его радиоактивности.

c) Аналогичным образом, облучение в реакторе топлива, изначально содержавшего уран с обогащением по ^{235}U не менее 10%, но не более 20% (например, топливо исследовательских реакторов, которое перед облучением обычно обогащается по ^{235}U примерно до 19,5%), как правило, не снизит обогащение по ^{235}U до менее чем 10%. Облучение топлива, обогащенного до таких уровней, не ведет к образованию количества плутония, превышающего установленные

для категории III пределы, из-за относительно малого объема топлива, используемого в исследовательских реакторах. Следовательно, категория такого топлива после облучения определяется в первую очередь на основе количества и степени обогащения. Таким образом, если общее количество такого топлива, находящегося в одном месте, содержит 10 кг или более ^{235}U до облучения, оно может быть перенесено из категории II в категорию III после облучения.

3.79. Возможность государства присвоить облученному топливу другую категорию физической защиты, отличную от указанной в таблице 1 (сноска d), необязательно относится к облученному топливу, которое изначально содержало некоторое количество плутония или урана категории I или II со степенью обогащения 10% и более. Уровень радиоактивности всех видов облученного топлива будет со временем снижаться, что может потребовать пересмотра категории материала, которому была присвоена более низкая категория на основании сноски е к строке 4 таблицы 1.

3.80. Как указано выше, в соответствии со сноской е к таблице 1 государства имеют возможность понизить на одну категорию меры физической защиты от несанкционированного изъятия ядерного материала, если такой ядерный материал имеет общую мощность дозы внешнего облучения, превышающую 1 Гр/ч на расстоянии 1 м от любой доступной поверхности без защиты (биологической). Указанный критерий — это мощность дозы, от которой лицо, пытающееся контактировать с таким материалом, начнет испытывать серьезный детерминированный эффект для здоровья от радиационного облучения в течение периода времени, составляющего менее 1 часа. При простом сценарии хищения изначально предполагалось, что мощность дозы радиации на таком уровне послужит эффективным средством сдерживания от хищения радиоактивного материала. Тем не менее некоторые современные нарушители доказали свою готовность рискнуть жизнью для исполнения своей миссии, и поэтому воздействие радиации от обращения с облученным топливом их, возможно, не остановит. В этой связи государствам следует внимательно задуматься над тем, является ли положение сноски е приемлемым с точки зрения коррекции их требований к обеспечению физической защиты.

Подходы к установлению дифференцированных требований по защите, основанных на форме или степени разбавления материала

3.81. Многие государства издавна используют трехфакторный метод для категоризации необлученного ядерного материала с целью применения надлежащих мер физической защиты от несанкционированного изъятия. В соответствии с данным методом для любого ядерного материала тремя факторами, которые учитываются при определении уровня физической защиты, требуемого для защиты от несанкционированного изъятия, являются делящийся элемент (плутоний или уран), изотопный состав и количество. Такой метод легко применять, но в некоторых случаях он может привести к излишнему ужесточению требований по защите материала. В этой связи предлагается, чтобы государство принимало во внимание другие характеристики материала, которые могут стать дополнительными препятствиями для нарушителя при потенциальных сценариях хищения; такие препятствия могут включать разбавление или широкое разделение ядерного материала.

3.82. В рекомендациях, содержащихся в [1], признается необходимость учета других факторов.

a) Для ядерного материала в целом категоризация, установленная в [1]:

   «служит основой для применения *дифференцированного подхода* в обеспечении защиты от *несанкционированного изъятия ядерных материалов,* которые могут применяться в ядерном взрывном устройстве, что, в свою очередь, зависит от типа ядерного материала (например, плутоний и уран), изотопного состава (т.е. содержания делящихся изотопов), физической и химической формы, степени разбавления, уровня излучения и количества» ([1], пункт 4.5).

b) Для отходов: «Защита от *несанкционированного изъятия ядерного материала,* который находится в форме, более не пригодной для использования в какой-либо ядерной деятельности, имеет минимальное рассеяние в окружающей среде и является практически нерегенерируемым, может быть обеспечена исходя из соображений практической целесообразности» ([1], пункт 4.7).
c) Для облученного топлива сноской e к таблице 1 допускается снижение категории на основании уровня излучения.

3.83. Из-за того, что ядерный материал находится в разбавленной форме, нарушитель будет стремиться завладеть намного большим количеством материала для получения значительного количества ядерного материала. Нарушителю также будет труднее получить ядерный материал ввиду необходимости применения более сложной технологической схемы для преобразования ядерного материала в форму, подходящую для изготовления ядерного взрывного устройства. Принимая во внимание указанные дополнительные трудности для нарушителя, государство может счесть целесообразным учитывать уровень разбавления при категоризации ядерного материала. Возможными дополнительными параметрами для категоризации могут быть концентрация ядерного материала и однородность концентрации внутри материала. Это может стимулировать переработку и хранение ядерных материалов в формах, менее привлекательных для нарушителя.

3.84. Если считается, что материал сам по себе изначально обладает свойствами, снижающими его привлекательность для нарушителя, или другими характеристиками, которые могут быть учтены при определении надлежащей защиты, то оценку вероятного эффекта от таких факторов следует произвести и задокументировать до того, как такие факторы будут использованы для коррекции мер физической защиты, определенных трехфакторным методом категоризации.

Дополнительные соображения, основанные на суммировании ядерного материала

> «4.8. При определении уровней физической защиты на установке, которая может состоять из нескольких зданий, *оператор* может, по согласованию с *компетентным органом* государства, выделить ту часть *ядерной установки*, в которой содержится *ядерный материал* другой категории и защита которой обеспечивается на ином уровне, чем остальные части *ядерной установки*. И наоборот, может потребоваться рассмотрение вопроса о сложении вместе общего количества *ядерного материала*, содержащегося в ряде зданий, с тем чтобы определить соответствующие меры защиты для этой группы зданий» [1].

3.85. При определении уровней физической защиты для ядерной установки, группы зданий или группы помещений от несанкционированного изъятия ядерного материала может быть применено агрегирование (сложение вместе) общего количества ядерного материала внутри установки, группы

зданий или группы помещений. Метод, используемый для агрегирования ядерного материала, является важным элементом работы по определению и, при необходимости, повышению требуемых уровней физической защиты.

3.86. В пункте 4.8 публикации [1] допускается возможность того, что во время одного нападения некоторое количество ядерного материала может быть изъято нарушителем из разных мест или зданий.

3.87. На некоторых установках ядерный материал одного типа (например, уран с обогащением по ^{235}U более 20%) может находиться в нескольких разных зданиях — для разных нужд или на разных этапах технологического процесса. Например, 4 кг такого материала могут находиться в одном здании, а другие 4 кг аналогичного материала — в другом здании в пределах той же защищенной зоны. Если считать по отдельности, то каждое количество материала будет отнесено к категории II. Однако если все 8 кг могут быть захвачены нарушителем во время одного нападения, то материал следует отнести к категории I и система физической защиты должна быть соответствующим образом усилена.

3.88. Ядерный материал других типов (например, плутоний, ^{233}U, уран с другой степенью обогащения по ^{235}U) может размещаться на одной и той же ядерной установке. При категоризации ядерного материала в любом конкретном месте внутри установки и, следовательно, при определении надлежащих мер физической защиты, применимых к этому ядерному материалу, должно учитываться общее количество ядерного материала на установке. Существует несколько возможных формул для определения категорий агрегированного количества разного ядерного материала, и государству следует решить, какой подход оно будет использовать. В одном из подходов к агрегированию разных типов ядерного материала используется набор формул, основанных на таблице 1: данный подход описан в приложении III.

3.89. Усиленная защита от несанкционированного изъятия из разных мест внутри ядерной установки может не потребоваться, если компетентный орган согласится с заключением оператора, что несанкционированное изъятие отдельных объемов материала из разных мест одним нарушителем маловероятно по следующим причинам:

а) отдельные места защищены отдельными системами физической защиты, и сотрудники охраны и/или силы реагирования способны эффективно противостоять нападениям нарушителей во всех местах;

b) отдельные места эксплуатируются и контролируются разными группами сотрудников, вследствие чего угроза со стороны внутреннего нарушителя ограничивается одним местом.

3.90. Оператор также может оценить, каким количеством ядерного материала нарушитель может завладеть за определенный период времени, для обоснования решения о том, какой уровень физической защиты может быть сочтен подходящим для агрегированного количества. После этого оператор должен a) предложить надлежащие меры физической защиты для уменьшения способности нарушителя агрегировать ядерный материал или b) применить надлежащие меры физической защиты, если агрегирование ядерного материала приводит к повышению категории.

Градация уровней физической защиты, основанная на последствиях саботажа (диверсии)

> «3.44. ...Для защиты от *саботажа (диверсий)* государству следует устанавливать пределы *неприемлемых радиологических последствий*, с тем чтобы определить соответствующий уровень физической защиты с учетом существующих мер ядерной безопасности или радиационной защиты» [1].

3.91. В отличие от категоризации ядерного материала для защиты от несанкционированного изъятия, описанной в таблице 1, простой схемы классификации целей саботажа (диверсии) не существует: категория, определенная для ядерного материала на основе риска несанкционированного изъятия, не годится в качестве показателя потенциальных последствий саботажа (диверсии) в отношении материала или установки, на которой находится материал. Например, свежее высокообогащенное урановое топливо (категория I) имеет большую значимость с точки зрения потенциального хищения, но весьма малую значимость с точки зрения саботажа (диверсии) ввиду низкого уровня радиоактивности данного материала и потенциальных радиологических последствий его выброса. Вместе с тем высокообогащенное урановое топливо, облученное в реакторе, может иметь меньшую значимость с точки зрения хищения, поскольку высокий уровень радиоактивности от продуктов деления и активации сделают хищение затруднительным и опасным, но может быть более привлекательным в качестве цели саботажа (диверсии) из-за потенциальных радиологических последствий выброса продуктов деления и активации.

3.92. Государству следует создать регулирующую основу физической защиты от саботажа (диверсии), которая должна включать определение государством предела неприемлемых радиологических последствий. Затем эта основа должна быть применена оператором при разработке мер физической защиты от саботажа (диверсии). Как указано в пунктах 3.93–3.95, государствам следует также установить предел серьезных радиологических последствий, при превышении которого рекомендуется выделить и поставить под более надежную защиту особо важные зоны, как это определено в [1], пункты 5.20–5.42.

Неприемлемые радиологические последствия и серьезные радиологические последствия

3.93. Потенциальные последствия саботажа (диверсии) сопоставляются с уровнем, выше которого радиологические последствия определяются государством как неприемлемые. Определение неприемлемых радиологических последствий может быть количественным или качественным. Неприемлемые радиологические последствия определяются государством и могут включать критерии выброса радионуклидов (например, общий выброс активности или выброс определенного(ых) радионуклида(ов) сверх определенного уровня), дозовые критерии (например, выброс, достаточный для того, чтобы доза радиации для лица в определенном месте превысила определенный предел) и проектные пределы (например, саботаж (диверсия), который может привести к существенному повреждению активной зоны реактора). Для всего радиоактивного материала на ядерных установках следует применять одни и те же критерии неприемлемости потенциальных радиологических последствий саботажа (диверсии). Сформулированное государством определение неприемлемых радиологических последствий, в свою очередь, позволит определить цели саботажа (диверсии), способного привести к таким последствиям, которые, таким образом, должны быть поставлены под защиту. Решение вопроса о том, какие последствия следует считать неприемлемыми радиологическими последствиями (и серьезными радиологическими последствиями; см. ниже), будет предполагать учет соображений ядерной безопасности и должно осуществляться в тесной консультации с органами по ядерной безопасности. Например, определения неприемлемых радиологических последствий и серьезных радиологических последствий могут быть связаны с критериями, используемыми для аварийной готовности и реагированию [10, 11].

3.94. Предел неприемлемых радиологических последствий может быть установлен на уровне, соответствующем относительно небольшому выбросу радионуклидов в локализованном месте внутри ядерной установки. Цели, которые могут привести только к таким незначительным последствиям, могут требовать соответственно низкого уровня защиты. С другой стороны, цели, саботаж (диверсия) в отношении которых может привести к существенному радиологическому выбросу, серьезно влияющему на население и окружающую среду вне границ ядерной установки, требуют наиболее высокого уровня защиты. Такое экстремальное событие, согласно [1], влечет за собой серьезные радиологические последствия.

3.95. Следовательно, государство должно также определить предел серьезных радиологических последствий. Если потенциальные радиологические последствия саботажа (диверсии) определены как равные пределу серьезных радиологических последствий или превышающие его, должны быть определены и поставлены под защиту особо важные зоны, как это рекомендовано в [1], пункты 5.20–5.42, при помощи процесса проектирования, описанного в [1], пункты 5.9–5.19. Если радиологические последствия попадают в промежуток между предельными значениями неприемлемых радиологических последствий и серьезных радиологических последствий, государство может установить дифференцированные требования по защите на основе потенциальных радиологических последствий и защита должна быть обеспечена при помощи процесса проектирования, описанного в [1], пункты 5.9–5.19. Если потенциальные радиологические последствия ниже предела неприемлемых радиологических последствий, оператору все равно следует предусмотреть защиту связанных с ядерной безопасностью устройств и оборудования посредством мер по контролю доступа к ним и их охраны, как это рекомендовано в [1], пункт 5.7. Соотношение между неприемлемыми радиологическими последствиями и серьезными радиологическими последствиями и уровнями защиты показано на рис. 1.

Диапазон потенциальных радиологических последствий саботажа (диверсии)

3.96. Оценка привлекательности целей саботажа (диверсии) для потенциальных нарушителей основывается на определенных государством пределах неприемлемых радиологических последствий и серьезных радиологических последствий и не зависит от категории ядерного материала, определенного на основании угрозы несанкционированного изъятия. Потенциальные радиологические последствия саботажа (диверсии)

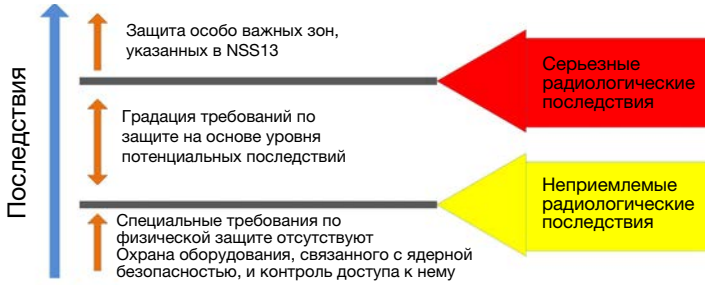

РИС. 1. Соотношение между неприемлемыми радиологическими последствиями и серьезными радиологическими последствиями и дифференцированными уровнями защиты. NSS13 — Серия изданий МАГАТЭ по физической ядерной безопасности, № 13.

будут зависеть от общего количества радиоактивного материала и легкости, с которой материал может быть рассеян (что, в свою очередь, будет зависеть от механизма рассеяния, запланированного в рамках саботажа (диверсии), и формы материала). Потенциальные радиологические последствия саботажа (диверсии) можно дифференцировать с учетом нескольких диапазонов тяжести, каждый из которых требует соответствующим образом дифференцированного уровня защиты.

3.97. Вероятность того, что акт саботажа (диверсии) приведет к неприемлемым радиологическим последствиям на ядерной установке, зависит от характеристик установки (например, типа установки и особенностей ее использования, проектирования, сооружения, эксплуатации и компоновки) и от самого акта саботажа (диверсии). Факторы, которые следует учитывать при определении того, возможно ли наступление неприемлемых радиологических последствий на установке, включают следующие характеристики (если применимо):

a) количество, тип, физическая форма и состояние радиоактивного материала на ядерной установке (например, твердая или жидкая форма, используется или хранится);
b) риск (например, достижения критичности), изначально присущий физическим и химическим процессам, которые обычно происходят на ядерной установке;
c) характеристики процессов или инженерно-технических средств, которые могут стать нестабильными при нападении;
d) тепловая мощность установки и история облучения ядерного топлива (для ядерного реактора);

e) конфигурация ядерной установки для разных видов деятельности;
f) пространственное распределение радиоактивного материала на ядерной установке. Например, на исследовательских реакторных установках основная часть наличного радиоактивного материала обычно находится в активной зоне реактора и бассейне выдержки топлива; на предприятиях по переработке и в хранилищах наличный радиоактивный материал может быть распределен по площадке;
g) характеристики ядерной установки, имеющие отношение к последствиям рассеяния радионуклидов в атмосфере и гидросфере (например, размер, проект и особенности строительства установки или демографический состав и наземный и водный ландшафт региона);
h) потенциальное радиологическое загрязнение за пределами площадки в сравнении с загрязнением на площадке (что частично будет зависеть от расположения радиоактивного материала относительно границ площадки).

3.98. Один из методов выработки дифференцированного подхода к защите от саботажа (диверсии) предполагает, что государство установит уровни радиационного облучения на границе ядерной установки как пределы неприемлемых радиологических последствий и серьезных радиологических последствий вместе с соответствующими уровнями эффективности, которые требуются от системы физической защиты радиоактивного материала, который в случае саботажа (диверсии) может повлечь радиологические последствия на таких уровнях. Оператор, в свою очередь, должен провести оценку всех возможных целей саботажа (диверсии) для определения в отношении каждой цели того, приведет ли рассеяние соответствующего наличного количества радиоактивного материала к радиологическим последствиям, превышающим эти установленные уровни. Результат такой оценки используется для определения уровней защиты, необходимых для разных зон установки, с учетом возможностей нарушителей.

3.99. В таблице 2 показан другой пример того, как провести градацию уровней физической защиты для разных диапазонов потенциальных радиологических последствий. Такой менее сложный подход служит отправной точкой для создания системы физической защиты от саботажа (диверсии) исходя из уровней последствий, соответствующих предлагаемым категориям аварийной готовности для установок и деятельности, описанным в документах Серии норм безопасности МАГАТЭ о готовности в случае ядерной или радиологической аварийной ситуации [10–12]. Таблица основана на допущении, что общее количество радиоактивного материала, которое может быть рассеяно во время саботажа

(диверсии), увеличивается с ростом уровня тепловой мощности реактора. Такой подход в большей степени подходит для предписывающего подхода к регулированию.

3.100. В таблице 2 выделены три пороговых значения потенциальных радиологических последствий саботажа (диверсии) как пример подхода к градации установок. Используя данную таблицу, государство может установить, что потенциальные радиологические последствия саботажа (диверсии) на атомной электростанции на уровне А являются серьезными радиологическими последствиями и требуют выделения особо важных зон [13]. Последствия уровней В и С представляют собой неприемлемые радиологические последствия, которые важны, но менее значимы по сравнению с серьезными радиологическими последствиями, и системы физической защиты для указанных уровней потенциальных последствий могут предполагать выделение защищенной зоны. Дополнительная информация о том, как определить потенциальные радиологические последствия саботажа (диверсии) на атомных электростанциях, представлена в [14]. Методы, описанные в [14], могут применяться и для других типов ядерных установок.

3.101. В публикации [8] рекомендуется, чтобы проектная угроза разрабатывалась и применялась всякий раз, когда государству требуется более твердая уверенность в том, что уровень физической защиты ядерного материала и ядерных установок достаточен для предотвращения неприемлемых радиологических последствий. В указанном примере проектная угроза должна использоваться при разработке мер защиты целей с последствиями уровня А, которые могут быть причиной серьезных радиологических последствий, как это рекомендовано в [1], пункт 3.37. Проектная угроза также может по усмотрению государства использоваться для целей с последствиями уровня В и целей с последствиями уровня С.

ТАБЛИЦА 2. ПРИМЕР ДИФФЕРЕНЦИРОВАННОГО ПОДХОДА К ТРЕБОВАНИЯМ ПО ЗАЩИТЕ ОТ САБОТАЖА (ДИВЕРСИИ)

Последствия уровня A	Последствия уровня B	Последствия уровня C*
Саботаж (диверсия) может привести к возникновению серьезного детерминированного эффекта для здоровья за пределами площадки, например: – установки с общим количеством способного к рассеянию радиоактивного материала, достаточным для того, чтобы повлечь за собой серьезный детерминированный эффект за пределами площадки – реакторы мощностью более 100 МВт (тепл.) (например, атомная электростанция, атомная подлодка, исследовательская установка) – бассейны выдержки отработавшего топлива, которые могут содержать некоторое количество недавно выгруженного топлива и в общей сложности более чем 0,1 ЭБк Cs-137 (эквивалент общего количества топлива в активной зоне реактора мощностью 3000 МВт (тепл.)	Саботаж (диверсия) может привести к облучению лиц за пределами площадки в дозах, требующих принятия срочных защитных мер за пределами площадки, например: – установки с общим количеством способного к рассеянию радиоактивного материала, достаточным для того, чтобы повлечь за собой дозы, требующие принятия срочных защитных мер за пределами площадки – реакторы мощностью 100 МВт (тепл.) или менее, но более 2 МВт (тепл.) – бассейны выдержки отработавшего топлива, требующие активного охлаждения – установки с возможностью неконтролируемой критичности в пределах 0,5 км от границ площадки	Саботаж (диверсия) может привести к облучению или радиоактивному загрязнению, требующим принятия срочных защитных мер на площадке, например: – установки с общим количеством способного к рассеянию радиоактивного материала, достаточным для того, чтобы повлечь за собой дозы, требующие принятия срочных защитных действий на площадке – установки с возможностью прямого облучения с мощностью внешней дозы более 100 мГр/ч на расстоянии 1 м, при потере защиты – установки с возможностью неконтролируемой критичности более чем в 0,5 км от границ площадки – реакторы мощностью 2 МВт (тепл.) или менее

*Потенциальные последствия ниже уровня C требуют организации защиты как минимум исходя из соображений практической целесообразности.

Глубокоэшелонированная защита[3]

> **«В требованиях государства к физической защите следует отразить концепцию нескольких эшелонов и методов защиты (конструкционных или других инженерно-технических, кадровых и организационных), которые требуется преодолеть или обойти нарушителю для достижения своих целей. (ОСНОВОПОЛАГАЮЩИЙ ПРИНЦИП I: *Глубокоэшелонированная защита)***
>
> 3.45. Требования государства по физической защите следует основывать на принципе *глубокоэшелонированной защиты*. Концепция физической защиты требует сочетания предусматриваемых проектом аппаратных средств (устройств, обеспечивающих физическую безопасность), процедур (включая организацию работы *сотрудников охраны* и выполнение ими своих обязанностей) и элементов конструкции установки (включая их компоновку)» [1].

3.102. Государству следует установить требование о применении концепции глубокоэшелонированной защиты при проектировании системы физической защиты для каждой ее функций: обнаружения, задержки и реагирования. Для каждой из этих функций в рамках системы следует предусмотреть независимые функциональные возможности для того, чтобы отказ одной функциональной возможности не означал потерю всей функции. Например, обнаружение может основываться на наблюдении, которое ведется персоналом, и/или использовании электронных средств. Задержка может обеспечиваться несколькими независимыми и неодинаковыми физическими барьерам, которые необходимо преодолеть для получения доступа к цели (такими как заграждения, баррикады и укрепленные здания). Реагирование может обеспечиваться сотрудниками охраны на площадке и местной полицией, равно как и силами реагирования на площадке и за пределами площадки.

---

[3] Согласно определению, данному в контексте физической ядерной безопасности в [1], в настоящей публикации термин «глубокоэшелонированная защита» используется для обозначения сочетания нескольких уровней систем и мер, которые необходимо преодолеть или обойти для нарушения физической защиты. Этим термином описывается концепция, в принципе схожая с «глубокоэшелонированной защитой» в ядерной безопасности, но необходимо отметить, что конкретное определение не совпадает с определением, используемым в Серии норм безопасности МАГАТЭ.

3.103. Совмещение дифференцированного подхода с применением глубокоэшелонированной защиты потребует применения большего количества уровней и более эффективных компонентов в рамках мер физической защиты (обнаружение, задержка и реагирование) целей для хищения, которым присвоены высокие категории, и целей для саботажа (диверсии) с более высоким уровнем потенциальных последствий.

ОБЕСПЕЧЕНИЕ УСТОЙЧИВОСТИ РЕЖИМА ФИЗИЧЕСКОЙ ЗАЩИТЫ

3.104. Обеспечение устойчивости государственного режима физической ядерной безопасности — один из основных элементов, указанных в публикации № 20 Серии изданий МАГАТЭ по физической ядерной безопасности «Цель и основные элементы государственного режима физической ядерной безопасности» [4]. Устойчивость зависит от элементов, которые способствуют надежному, эффективному режиму физической ядерной безопасности. В [1] выделены четыре элемента, которые в особенной степени способствуют устойчивости системы физической защиты:

a) культура физической ядерной безопасности: определение культуры физической ядерной безопасности прямо включает фразу «устойчивое сохранение физической ядерной безопасности»;
b) обеспечение качества: процесс, дающий уверенность в том, что требования физической защиты выполняются на постоянной основе;
c) конфиденциальность: предотвращение разглашения чувствительной информации, которая может поставить под угрозу физическую защиту;
d) программа обеспечения устойчивости: программа, которая специально посвящена техническому обслуживанию, ресурсам и инфраструктуре — финансовой, кадровой и технической,— необходимым для эффективной физической защиты.

Культура физической ядерной безопасности

> **«Всем организациям, занимающимся вопросами осуществления физической защиты, следует уделять должное внимание культуре физической безопасности, ее развитию и поддержанию как необходимым факторам для ее эффективного осуществления во всей организации. (ОСНОВОПОЛАГАЮЩИЙ ПРИНЦИП F: Культура физической ядерной безопасности)**» [1].

3.105. Руководящие указания по культуре физической ядерной безопасности содержатся в публикации [15], в которой культура физической ядерной безопасности определена как «совокупность характеристик, отношения к делу и поведения людей, организаций и учреждений, посредством которых обеспечивается поддержание, повышение и устойчивое сохранение физической ядерной безопасности».

3.106. Формирование высокой культуры физической ядерной безопасности потребует участия людей из различных сфер деятельности и организаций, которые должны работать сообща, чтобы добиться результата. Все организации должны придерживаться государственной политики в области физической ядерной безопасности, разработанной в соответствии с законодательной и регулирующей основой государства. Организациям необходимо создать надлежащие управленческие структуры, выделить достаточные ресурсы и ввести в действие соответствующие системы управления. Руководители данных организаций призваны играть ключевую роль в укреплении культуры посредством практики лидерства и менеджмента, которая включает в себя мотивацию персонала и постоянное стремление к совершенствованию. Результатом эффективного внедрения культуры физической ядерной безопасности станет применение всеми сотрудниками строгого и разумного подхода к физической защите, бдительность, критическая позиция и быстрое и корректное реагирование, если в нем возникнет необходимость.

Обеспечение качества

«В целях обеспечения уверенности в том, что требования, определенные для всех важных с точки зрения физической защиты видов деятельности, удовлетворены, следует установить и осуществлять политику и программы обеспечения качества. (ОСНОВОПОЛАГАЮЩИЙ ПРИНЦИП J: Обеспечение качества)

3.52. «Следует предусматривать, чтобы политика и программы обеспечения качества в области физической защиты обеспечивали, чтобы *система физической защиты* проектировалась, создавалась, функционировала и поддерживалась в состоянии, в котором она способна обеспечивать эффективное реагирование в отношении *оценки угроз* или *проектной угрозы*, и чтобы она удовлетворяла требованиям регулирующих правил государства, включая предписывающие и/или ориентированные на достижение определенных показателей требования» [1].

3.107. Программа обеспечения качества — это механизм получения данных через какой-либо процесс или систему, систематического сличения полученных данных со стандартами и мониторинга процесса или системы. Цель данной программы — сведение к минимуму ошибок и недоработок. Обеспечение качества является одним из элементов интегрированной системы менеджмента.

3.108. Для того чтобы созданная система физической защиты постоянно была эффективной, компетентному органу и операторам предлагается:

a) постоянно применять аспекты обеспечения качества политики и программы управления в части физической защиты ядерного материала и ядерных установок от несанкционированного изъятия и саботажа (диверсии);
b) в программных документах сообщить о своих обязанностях по обеспечению качества и разъяснить их, чтобы продемонстрировать свою приверженность этому делу и, при необходимости, дать руководящие указания персоналу, изложив цели организации по качеству;
c) спланировать программу управления таким образом, чтобы предусмотреть прямую подотчетность за обеспечение качества перед высшим руководством организации;
d) разработать для своих соответствующих организаций такие программы управления, которые предусматривают выявление и оценку недостатков, а также составление и отслеживание планов корректирующих мер.

3.109. Предполагается, что имеющиеся у операторов программы управления будут обеспечивать, чтобы у систем физической защиты, нацеленных на выполнение требований, ориентированных на достижение определенных показателей, имелись соответствующие документы, подтверждающие их эффективность. Эта информация особенно важна при определении компенсирующих мер и применении корректирующих мер. Такие программы также должны обеспечивать, чтобы о событиях, связанных с физической ядерной безопасностью, своевременно сообщалось компетентному органу (см. пункты 3.47 и 3.48).

3.110. Кроме того, рекомендуется, чтобы программы управления охватывали всю деятельность, связанную с физической безопасностью (техническую, процедурную и административную), и периодически пересматривались и актуализировались. Программы управления играют

важную роль в управлении конфигурацией системы физической защиты для обеспечения бесперебойной работы таких систем и обоснования решений о внесении изменений.

Конфиденциальность

> **«Государству следует установить требования в отношении защиты конфиденциальной информации, несанкционированное раскрытие которой может поставить под угрозу физическую защиту *ядерного материала* и *ядерных установок*. (ОСНОВОПОЛАГАЮЩИЙ ПРИНЦИП L: Конфиденциальность)**
>
> 3.53. Государству следует принимать меры по обеспечению надлежащей защиты конкретной или детальной информации, несанкционированное раскрытие которой может поставить под угрозу физическую защиту *ядерных материалов* и *ядерных установок*. Используя *дифференцированный подход*, государству следует определить, какую информацию необходимо защищать и как это следует делать» [1].

3.111. Руководящие указания по информационной безопасности для государств содержатся в [16]. В соответствии с ними:

> «2.5. Чувствительная информация — это информация, несанкционированное раскрытие (или корректировка, изменение, уничтожение или неиспользование) которой может поставить под угрозу физическую ядерную безопасность или другим способом содействовать совершению злоумышленного действия в отношении ядерной установки, организации или транспорта. Такая информация может касаться, например, обеспечения физической ядерной безопасности на установке, конструкций, систем и элементов на установке, местоположения и данных о перевозке (транспортировке) ядерных материалов или других радиоактивных материалов, а также данных персонала организации».

3.112. Государство устанавливает требования по информационной безопасности, которые должны соблюдаться оператором; данные требования должны быть основаны на инструкциях и политике органов национальной безопасности. Государство определяет, что следует считать чувствительной информацией, и на основе дифференцированного подхода устанавливает соответствующие требования по информационной безопасности для владельцев такой информации. Пример схемы классификации информации по вопросам физической ядерной безопасности приведен в [16].

3.113. Защита конфиденциальности и обеспечение доступности и сохранности информации зависит от применения мер защиты чувствительной информации, чтобы такая информация не была получена или изменена лицами или организациями, не имеющими на это полномочий. Информационная безопасность включает системы, программы и набор правил, которые обеспечивают защиту информации в любой форме. Информационная безопасность включает как минимум следующее:

a) защиту информации на физических и электронных носителях;
b) защиту компьютерных систем (компьютерную безопасность);
c) защиту систем связи и сетей;
d) защиту информации о работниках установки и третьих лицах (например, подрядчиках и поставщиках);
e) защиту недокументированной информации (например, знаний о вышеперечисленном).

3.114. Организации, обладающие чувствительной информацией, должны обеспечивать проведение в жизнь государственной политики в области информационной безопасности, а также полную осведомленность всех работников о важности безопасности и соблюдение ими правил организации.

3.115. Каждая организация должна разработать внутреннюю политику, планы и процедуры по защите конфиденциальности, целостности и доступности своей чувствительной информации в соответствии с национальной политикой в области информационной безопасности.

3.116. Пункт 3.54 публикации [1] гласит:

> «Руководству, ответственному за *систему физической защиты*, следует принимать меры по ограничению доступа к чувствительной информации и предоставлять ее только тем сотрудникам, чья благонадежность после проверки была признана приемлемой для получения доступа к такой информации и которым ее необходимо знать для выполнения своих служебных обязанностей. Следует обеспечивать надежную защиту информации о возможных уязвимых местах в *системах физической защиты*».

Информация, подлежащая защите, может включать данные о местоположении и характеристики целей для саботажа (диверсии) и хищения, информацию о конструкции и эксплуатации системы физической

защиты — включая возможные уязвимые места в системе защиты и некоторые аспекты учета и контроля ядерного материала — и данные о тактике и действиях сил реагирования в плане чрезвычайных мер.

3.117. Государству следует четко прописать положения, которым должен следовать оператор при обеспечении конфиденциальности информации, касающейся системы физической защиты. В таких положениях должны быть определены информация, нуждающаяся в защите, и необходимый уровень защиты, соразмерный степени чувствительности информации и последствиям ее потери. Меры оператора по соблюдению указанных положений следует отразить в плане обеспечения физической безопасности оператора и периодически оценивать оператором и компетентным органом.

3.118. Пункт 3.55 публикации [1] гласит: «В законодательную или регулирующую систему государства следует включать санкции, применяемые к лицам, нарушающим режим конфиденциальности». Информация о санкциях против лиц, нарушающих режим конфиденциальности, должна быть доведена до сведения лиц, которым официально предоставлен доступ к чувствительной информации, и эти санкции должны быть достаточно строгими для того, чтобы удерживать персонал от таких действий. Государства должны установить за такие правонарушения соответствующие наказания с учетом их потенциальной тяжести.

Программа обеспечения устойчивости

3.119. Государству следует обеспечить, чтобы законодательная и регулирующая основа способствовала устойчивости инфраструктуры, систем и мер физической защиты как части режима физической ядерной безопасности. Две положительные практики для государства состоят в том, чтобы создать инфраструктуру для обучения персонала как государственных органов, так и оператора по вопросам физической защиты и, если это практически возможно, предоставить материальную базу для испытаний и оценки оборудования физической защиты. Такие испытания могут дать государству и операторам информацию о практических способах поддержания мер и оборудования физической защиты на надлежащем уровне эффективности.

ПЛАНИРОВАНИЕ МЕРОПРИЯТИЙ, ГОТОВНОСТЬ НА СЛУЧАЙ СОБЫТИЙ, СВЯЗАННЫХ С ФИЗИЧЕСКОЙ ЯДЕРНОЙ БЕЗОПАСНОСТЬЮ, И РЕАГИРОВАНИЕ НА ТАКИЕ СОБЫТИЯ

> **«В целях принятия ответных мер в случае *несанкционированного изъятия ядерного материала* или *саботажа (диверсии)* в отношении *ядерных установок* или *ядерного материала* или попыток таких действий должны быть подготовлены *планы чрезвычайных мер* (планы аварийных мероприятий), которые должны надлежащим образом отрабатываться всеми соответствующими обладателями лицензий и компетентными органами. (ОСНОВОПОЛАГАЮЩИЙ ПРИНЦИП K: *Планы чрезвычайных мер*)»** [1].

3.120. Этот основополагающий принцип может навести на мысль, что планы чрезвычайных мер и планы аварийных мероприятий — это одно и то же. На самом деле государства по-разному определяют и используют эти термины. В [1] план чрезвычайных мер является частью общего плана физической ядерной безопасности и касается реагирования персонала по вопросам физической защиты на события, связанные с физической ядерной безопасностью, при совершении злоумышленных действий. В документе № GSR Part 7 Серии норм безопасности МАГАТЭ «Готовность и реагирование в случае ядерной или радиологической аварийной ситуации» [10] план аварийных мероприятий касается реагирования на ядерные или радиологические аварийные ситуации, будь то в результате аварии или злоумышленных действий. Тем не менее применение плана чрезвычайных мер и плана аварийных мероприятий требует согласованного реагировании сотрудников по вопросам физической защиты, учета и контроля ядерного материала и ядерной безопасности.

3.121. Во время реагирования на событие, связанное с физической ядерной безопасностью, необходимо, чтобы все организации, участвующие в реагировании, были готовы принять надлежащие меры на местном и национальном уровне. Меры, которые следует принимать государству для планирования, подготовки к событию, связанному с физической ядерной безопасностью, и реагированию на него, описаны в [4]. У государства и оператора есть общие и взаимодополняющие обязанности по планированию, подготовке к событиям, связанным с физической ядерной безопасностью, и реагированию на них, которые состоят в обнаружении и возвращении пропавших ядерных материалов и смягчении или сведении к минимуму последствий саботажа (диверсии). Что касается действий по обнаружению и возвращению ядерных материалов после хищения, то

оператор может иметь ограниченные полномочия за пределами ядерной установки, и поэтому главную ответственность за реагирование на такие события за пределами площадки будет, скорее всего, нести государство. В этой связи между оператором и государственными организациями должны быть четко распределены обязанности.

3.122. Цели планирования чрезвычайных мер состоят в обеспечении своевременного и эффективного реагирования на всех уровнях на любое событие, связанное с физической ядерной безопасностью, включая злоумышленное действие, направленное на ядерную установку или связанное с ней, а также в поддержании режима физической защиты во время других событий, таких как авария с выбросом радионуклидов, чрезвычайная медицинская ситуация или стихийное бедствие. Для адекватного реагирования на событие и разрешение ситуации необходимо принять правильные меры и своевременные решения. В случае ядерной или радиологической аварийной ситуации следует принять меры к тому, чтобы обеспечить непрерывную эффективность системы физической защиты в ходе реализации плана аварийных мероприятий.

3.123. Государству и компетентному органу следует обеспечить, чтобы план чрезвычайных мер, входящий в план обеспечения физической безопасности оператора, соответствовал аналогичному плану, составленному на государственном уровне. Этому может способствовать разработка соглашений (документы в письменной форме, такие как меморандум о взаимопонимании или другие протоколы) между государственными органами, вовлеченными в реагирование, и оператором; в этих соглашениях будут, к примеру, четко прописаны функции и обязанности каждой организации. Необходимый уровень координации можно обеспечить, например, путем организации совместной подготовки и учений с использованием практических сценариев и надлежащих планов чрезвычайных мер.

3.124. У государства, соответствующих компетентных органов и оператора должен иметься полный набор планов чрезвычайных мер для разных типов событий, связанных с физической ядерной безопасностью. Примеры таких событий, которые могут требовать плана чрезвычайных мер, приведены в приложении 1.

3.125. Государству следует обеспечить регулярное проведение учений для подтверждения эффективности планов чрезвычайных мер в рамках общего режима физической ядерной безопасности. Такие учения должны включать сценарии как несанкционированного изъятия, так и саботажа (диверсии), которые входят в оценку угроз или проектную угрозу.

3.126. Дополнительные руководящие указания по надлежащему реагированию для обнаружения и возвращения ядерных материалов, находящихся вне регулирующего контроля (например, в результате хищения), представлены в [7].

4. РАЗРАБОТКА, ВНЕДРЕНИЕ И ОБЕСПЕЧЕНИЕ ФУНКЦИОНИРОВАНИЯ ИНТЕГРИРОВАННОЙ СИСТЕМЫ ФИЗИЧЕСКОЙ ЗАЩИТЫ ЯДЕРНЫХ УСТАНОВОК

4.1. Данный раздел содержит руководящие указания для оператора по применению «Рекомендаций» [1], касающихся физической защиты ядерного материала и ядерных установок от несанкционированного изъятия и саботажа (диверсии). Такие рекомендации в целом изложены в пунктах 3.23–3.30 и разделах 4 и 5 публикации [1].

4.2. В [1] рекомендуется, чтобы требования по обеспечению физической защиты как от несанкционированного изъятия ядерного материала, так и от саботажа (диверсии) применялись в комплексе, т.е. чтобы система физической защиты была единой системой, эффективной против обеих угроз. Кроме того, в [1] рекомендуется проектировать систему физической защиты таким образом, чтобы обеспечить эффективное реагирование на любой риск — несанкционированного изъятия или саботажа (диверсии), — что требует применения более жестких требований по обеспечению физической защиты ([1], пункты 4.4, 5.3 и 5.17).

4.3. В данном разделе описан предлагаемый подход к проектированию единой системы физической защиты, эффективной против угрозы как несанкционированного изъятия, так и саботажа (диверсии). В представленном в данном разделе поэтапном подходе к проектированию применены принципы системной разработки мер физической защиты — определение требований к физической защите, проектирование систем

для выполнения этих требований и оценка эффективности созданной системы физической защиты, — которые детально в [1] не освещаются. Могут существовать и другие способы определить элементы системного подхода к разработке мер физической защиты, но процедура, описанная в данном разделе, соответствует методологии, поддерживаемой МАГАТЭ, и призвана дать пользователям основные ориентиры для проектирования и внедрения системы физической защиты.

ОБЩИЕ ОБЯЗАННОСТИ ОПЕРАТОРА

> **«Следует четко определить обязанности по реализации различных элементов физической защиты в государстве. Государству следует обеспечить, чтобы основная ответственность за осуществление физической защиты *ядерного материала* и *ядерных установок* была возложена на обладателей соответствующих лицензий или других разрешительных документов (например, на *операторов* или *грузоотправителей*). (ОСНОВОПОЛАГАЮЩИЙ ПРИНЦИП E: Ответственность обладателей лицензий)»**
>
> .....
>
> «3.25. *Оператору, отправителю* и перевозчику следует сотрудничать и координировать свои действия со всеми другими органами (организациями) государства, несущими ответственность за обеспечение физической защиты, такими как *силы реагирования* за пределами площадки» [1].

4.4. При выполнении указанных обязанностей оператору следует полностью соблюдать положения законодательной и регулирующей основы государства. Эти положения могут обязывать оператора заключить соглашения (такие как меморандум о взаимопонимании, протоколы или другие виды документов в письменной форме) с местными правоохранительными органами, национальной полицией, армией и другими организациями, такими как местные и национальные службы аварийного реагирования, служба разведки и другие национальные силовые структуры.

4.5. Основная ответственность за разработку и внедрение системы физической защиты ядерных материалов на своей установке лежит на операторе. Оператору следует разработать план обеспечения физической безопасности для конкретной установки (см. пункты 4.154–4.161). Предлагаемый формат плана обеспечения физической безопасности представлен в приложении 1.

4.6. Пункт 3.30 публикации [1] гласит:

> «Если устанавливается, что *система физической защиты* не способна обеспечить необходимый уровень защиты, *оператору, отправителю* и/или перевозчику следует незамедлительно предпринять компенсирующие меры в целях обеспечения надлежащей защиты. *Оператору* и/или *отправителю* следует затем в течение согласованного срока спланировать и предпринять корректирующие меры, подлежащие рассмотрению и утверждению *компетентным органом*».

Компенсирующие меры — это краткосрочные меры, которые принимаются для компенсации сниженной эффективности или неисправности конструкций, систем и элементов физической безопасности до тех пор, пока их не отремонтируют или не заменят. Один из подходов к обеспечению компенсирующих мер — увеличение численности сотрудников охраны и/или сил реагирования для компенсации указанных недостатков сразу же после их обнаружения. Предлагается документировать и утверждать компенсирующие меры, а также согласовывать механизмы необходимой координации между государством, компетентным органом, оператором и силами реагирования до принятия таких мер.

4.7. Пункт 3.28 публикации [1] гласит:

> «В случае *новой ядерной установки* соображения, касающиеся обеспечения физической защиты, следует учитывать как можно раньше при выборе площадки и на стадии проектирования, а также следует рассматривать взаимодействие физической защиты, безопасности и учета и контроля ядерных материалов во избежание коллизий и в целях обеспечения того, чтобы все три элемента дополняли друг друга».

При выборе площадки для ядерных установок должны внимательно учитываться возможные последствия этого выбора с точки зрения физической ядерной безопасности. На физическую ядерную безопасность могут повлиять и местная инфраструктура, и планировка площадки, и другие условия местности. Планировка площадки, особенно для ядерных

объектов с несколькими ядерными установками, может потребовать дополнительного пространства для организации физической защиты, с тем чтобы создать надлежащую глубокоэшелонированную защиту.

4.8. Проектом новой ядерной установки также должны учитываться потребности физической защиты. Подход к проектированию для достижения этих целей называют «учетом требований безопасности при проектировании». Применение такого подхода может привести к уменьшению затрат на физическую защиту в течение срока службы ядерной установки и упростить задачу поддержания эффективности системы физической защиты в течение этого срока.

4.9. Суть учета требований безопасности при проектировании состоит в проектировании новой ядерной установки так, чтобы требуемый уровень безопасности был обеспечен наиболее экономичным способом, совместимым с эксплуатацией, ядерной безопасностью и учетом и контролем ядерного материала. Требования безопасности при проектировании лучше всего учитывать посредством структурированного подхода, при котором цели физической ядерной безопасности государства учитываются и полностью принимаются в расчет при принятии проектных решений в течение всего срока службы установки — от этапа планирования установки до этапов проектирования, сооружения, эксплуатации и вывода из эксплуатации.

4.10. Положительной практикой считается интеграция проекта системы физической защиты в общий проект ядерной установки на возможно более раннем этапе. Учет на ранних этапах предполагает принятие решений о выборе площадки и планировке объекта с учетом того, каким образом такие решения повлияют на проектирование и эффективность систем физической защиты. Важно свести к минимуму противоречия с другими проектными требованиями, используя возможности для взаимодополняемости и синергии при проектировании, например исключив потенциально уязвимые места благодаря подходящим инженерным решениям.

4.11. Высшие управляющие органы оператора должны быть осведомлены об интеграции мер физической защиты в процесс эксплуатации установки и дать добро на такую интеграцию.

Не менее важно, чтобы руководство поощряло высокую культуру физической ядерной безопасности, о чем говорится в [15] и вкратце упоминается в пунктах 3.105 и 3.106.

4.12. Чтобы комплексно подойти к внедрению системы физической защиты, оператор ядерной установки определяет все потенциальные цели несанкционированного изъятия и саботажа (диверсии) и вводит все требуемые защитные меры с использованием дифференцированного метода на основе государственного подхода к регулированию. В зависимости от типа ядерной установки цели саботажа (диверсии) либо цели несанкционированного изъятия могут требовать более высокого уровня защиты, но во всех случаях ко всем целям должен быть применен надлежащий уровень защиты. Именно такой подход подразумевается в рекомендации относительно «более жестких из применимых требований» в [1], пункты 4.4 и 5.3.

4.13. Вопросы физической ядерной безопасности при сооружении ядерных установок отдельно в «Рекомендациях» [1] не освещаются. Тем не менее положительная практика состоит в том, что оператору (или заявителю) следует до начала строительных работ определить, как будет обеспечиваться физическая защита на всех этапах строительства. Если рядом с площадкой, на которой планируется построить новую установку, уже находится ядерная установка, то до начала строительства обоим операторам в тесном взаимодействии друг с другом следует определить и ввести в действие любые дополнительные меры физической защиты существующей, уже эксплуатируемой установки. (Аналогичным образом, если ведутся строительные работы для расширения или модификации существующей ядерной установки, следует принять дополнительные меры для физической защиты существующих частей данной установки.) Для защиты от саботажа (диверсии) может также использоваться аудит ядерной безопасности и обеспечения качества, позволяющий обнаружить любые действия, призванные облегчить будущий саботаж (диверсию), такие как умышленное создание дефектов или внедрение скрытых устройств. В конце этапа строительства рекомендуется провести окончательную оценку для подтверждения эффективности мер физической защиты, прежде чем установка будет введена в эксплуатацию.

ОРГАНИЗАЦИОННОЕ ОБЕСПЕЧЕНИЕ ФИЗИЧЕСКОЙ БЕЗОПАСНОСТИ

4.14. Функции и обязанности в области физической безопасности следует определить в рамках интегрированной системы менеджмента, и они могут быть разделены между тремя следующими взаимодополняющими подразделениями.

a) Подразделение по управлению безопасностью, которое несет общую ответственность за физическую защиту и включает в свой состав руководителей, которые взаимодействуют с компетентным органом и руководством установки (включая руководителей кадровых служб), сотрудников по планированию, которые несут ответственность за составление и ведение плана обеспечения физической безопасности, проектировщиков, которые несут ответственность за проектирование или модернизацию системы физической защиты для выполнения требований компетентного органа, и аналитиков, которые несут ответственность за оценку соответствия работы системы физической защиты проектным требованиям. Распределение поручений, имеющих отношение к взаимосвязи между безопасностью и физической безопасностью, также входит в обязанности подразделения по управлению безопасностью (см. пункты 4.147–4.153).

b) Оперативное подразделение, которое несет ответственность за безопасность, связанную с персоналом и посетителями (проверка благонадежности и контроль доступа), информационную безопасность, компьютерную безопасность и работу охраны и сил реагирования (в соответствии с обязанностями, определенными государством), в чьи обязанности входит контроль доступа и сопровождение, функционирование центральной станции тревожной сигнализации, патрулирование и реагирование на события, связанные с физической ядерной безопасностью.

c) Техническое подразделение, включающее в свой состав технический персонал, который проводит установку и модернизацию, а также проверку рабочих характеристик оборудования (во взаимодействии с оперативным подразделением, если это необходимо), профилактический ремонт, внеплановый ремонт и замену оборудования; по мере необходимости подразделение также оказывает поддержку и предоставляет необходимые данные подразделению по управлению безопасностью и оперативному подразделению.

ПРОЦЕСС РАЗРАБОТКИ И ВНЕДРЕНИЯ СИСТЕМЫ ФИЗИЧЕСКОЙ ЗАЩИТЫ

4.15. В настоящем разделе описан подход к проектированию, разработке и внедрению системы физической защиты при строительстве новой ядерной установки (или сооружении новых объектов на существующих ядерных установках), модернизации действующих систем физической защиты и анализу эффективности действующих систем физической защиты.

Подход к разработке системы физической защиты

4.16. Разработка системы физической защиты наиболее эффективна при использовании системного подхода, который состоит из трех этапов. Это следующие этапы:

1) определение целей и требований к системе физической защиты;
2) проектирование системы физической защиты в соответствии с целями и требованиями, определенными на этапе 1;
3) анализ и оценка эффективности системы физической защиты, спроектированной на этапе 2, с точки зрения достижения целей и соблюдения требований, определенных на этапе 1.

Последовательность этих трех этапов и краткое описание мероприятий в рамках каждого этапа приведены на рис. 2.

4.17. Итогом работы на этих трех этапах, которые описываются более детально ниже в пунктах 4.23–4.59, станет проект системы физической защиты, обеспечивающий защиту от угроз несанкционированного изъятия и саботажа (диверсии) в отношении ядерного материала, а также решение всех других задач, которые могут быть поставлены для данной установки.

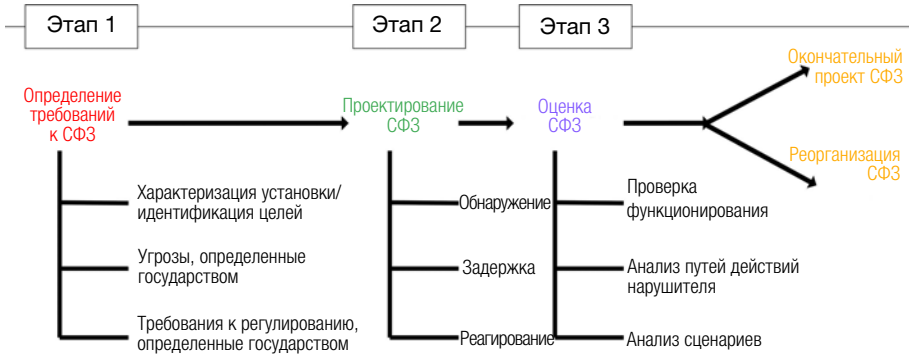

РИС. 2. Процесс проектирования и оценки системы физической защиты. СФЗ — система физической защиты.

Жизненный цикл системы физической защиты

4.18. После проектирования и оценки системы физической защиты в ходе данного процесса разработки следующими этапами жизненного цикла системы физической защиты являются реализация проекта; эксплуатация, техническое обслуживание и содержание созданной системы физической защиты; планирование соответствующей реорганизации системы физической защиты исходя из изменений в угрозе, конфигурации установки, эксплуатации или потенциальных целях либо на основе оценки функционирования. Указанные этапы жизненного цикла проиллюстрированы на рис. 3.

Обеспечение устойчивости системы физической защиты

«3.57. *Операторам*... следует разрабатывать и применять программы обеспечения устойчивости для своих *систем физической защиты*. В программы обеспечения устойчивости следует включать:

— эксплуатационные процедуры, регламенты (инструкции);
— управление людскими ресурсами и обучение;
— модернизацию, обслуживание, ремонт и калибровку оборудования;
— *проверку функционирования* и оперативный мониторинг;
— управление конфигурацией (процесс определения и документального оформления характеристик *системы физической защиты* установки, в том числе компьютерных систем и программного обеспечения, а также обеспечения того, чтобы изменения, вносимые в эти характеристики,

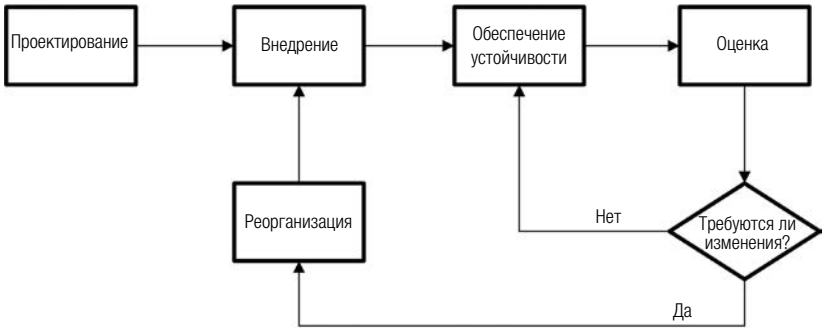

РИС. 3. Жизненный цикл системы физической защиты.

были должным образом проработаны, оценены, утверждены, выпущены, введены, проверены, зарегистрированы и включены в документацию установки);

— распределение ресурсов и анализ оперативных затрат» [1].

4.19. Принимая во внимание государственный подход к обеспечению устойчивости режима физической ядерной безопасности, операторы должны обеспечить выделение необходимых ресурсов — обученного и компетентного персонала, надежного оборудования, сопутствующей инфраструктуры, средств обеспечения качества и финансирования — для обеспечения устойчивости их систем физической защиты в рамках программы обеспечения устойчивости.

Соблюдение требований государства

4.20. До начала трехэтапного процесса, проиллюстрированного на рис. 2, оператору или заявителю следует получить представление о соответствующих аспектах государственного режима физической ядерной безопасности, о чем говорится в разделе 3. Особое значение имеет ряд аспектов, которые влияют на то, как оператор или заявитель проектирует систему физической защиты и представляет проект на утверждение государству. Это следующие аспекты:

a) законодательная и регулирующая основа государства, включая подход к регулированию, выбранный государством для установления требований по противодействию угрозе, о чем говорится в пунктах 3.12–3.26, и применение государственной политики проверки благонадежности;
b) требования, определенные государством на основе дифференцированного подхода, о чем говорится в пунктах 3.70–3.73;
c) процедура лицензирования для утверждения заявлений на получение новых лицензий и возобновление или изменение существующих лицензий, о чем говорится в пунктах 3.33–3.37.

4.21. В зависимости от принятого государством подхода к регулированию — подхода, ориентированного на достижение определенных показателей, предписывающего подхода или комбинированного подхода (описанных в пунктах 3.18–3.26) — оператор или заявитель могут по-разному подходить к соблюдению требований.

4.22. На рис. 4 показаны задачи, которые должны быть выполнены оператором или заявителем в зависимости от подхода к регулированию. При комбинированном подходе в определенных случаях потребуется решить обе группы задач. На рис. 3 показано, как проект разрабатывается и оценивается; рис. 4 описывает другие действия, которые выполняет оператор или заявитель, и согласования со стороны государства.

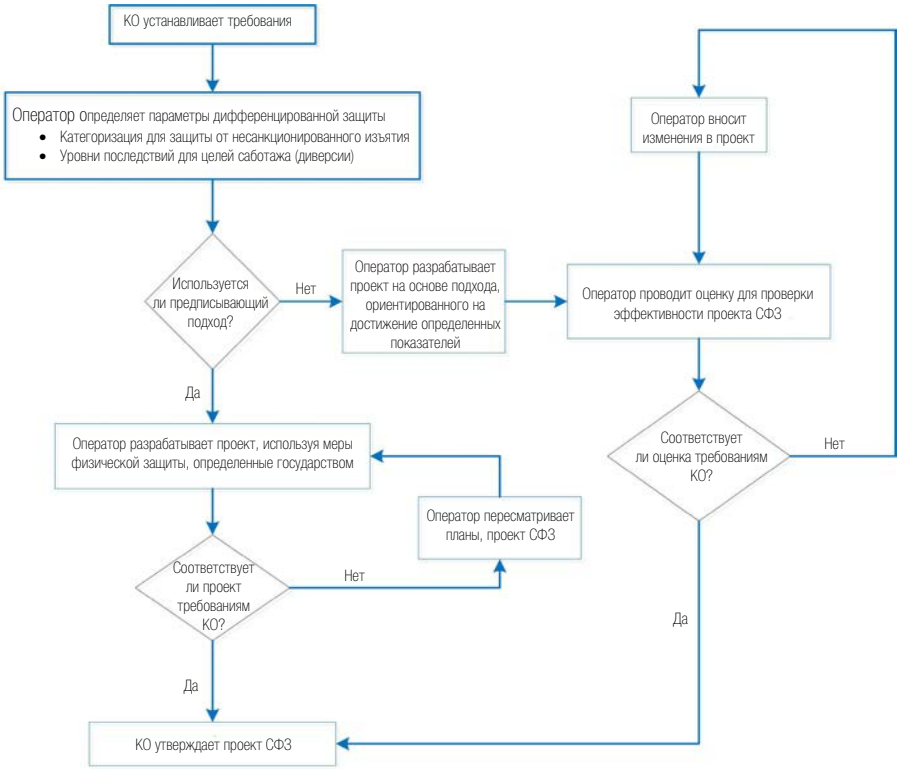

РИС. 4. Процесс проектирования системы физической защиты. КО — компетентный орган; СФЗ — система физической защиты.

ОПРЕДЕЛЕНИЕ ТРЕБОВАНИЙ К СИСТЕМЕ ФИЗИЧЕСКОЙ ЗАЩИТЕ (ЭТАП 1)

4.23. На этапе 1 разработки и оценки проекта системы физической защиты оператором или заявителем необходимо определить, каким образом применить требования государства в области физической защиты к конкретной площадке, ядерной установке и системе физической защиты. Для этого оператору или заявителю необходимо выполнить несколько шагов.

a) определение характеристик операций и условий на установке. Данный шаг включает описание процессов и операций на установке; разработку подробного описания установки, включая местоположение границ установки и зданий, поэтажный план, высоту зданий и мест прохода; для существующей установки или проекта — определение существующих конструктивных особенностей или систем, которые могут быть использованы как элементы системы физической защиты. Информация об установке может быть получена из всех соответствующих источников, включая имеющуюся документацию, такую как чертежи установки и описания процессов, а также наблюдения на объекте и опрос персонала. Проектировщикам системы физической защиты потребуется детально ознакомиться с этой информацией, а также со всеми ограничениями конкретной установки (такими как ограничения в части ядерной безопасности), которые могут помешать проектированию.
b) Интерпретация информации об угрозе, полученной оператором или заявителем от государства, которая послужит основой для проектирования (см. пункты 3.55–3.63). Данный шаг предусмотрен для подхода, ориентированного на достижение определенных показателей, и комбинированного подхода. (В рамках предписывающего подхода государство обычно не предоставляет оператору информацию об угрозах.)
c) Определение целей, которые необходимо защищать от нарушителя, и их местоположения на установке, как это определено государством на основе категоризации ядерного материала и/или потенциальных последствий саботажа (диверсии) (см. пункты 3.74–3.101).

4.24. Возможности нарушителя, определенные государством, должны быть нейтрализованы системой физической защиты, и поэтому их необходимо принимать в расчет оператору или заявителю. Эти возможности включают:

a) знание системы физической защиты;

b) навыки, которые будут полезными при нападении;
c) инструменты и оружие, которые могут быть использованы при нападении.

Определение целей

4.25. В ходе определения целей выясняется, какой материал и/или оборудование необходимо защитить от нарушителя. В процессе определения целей выделяются четыре шага:

a) уяснение целей физической защиты;
b) определение типов ядерного и другого радиоактивного материала, а также важных для безопасности систем (включая компьютерные системы и информацию), которые необходимо защитить от несанкционированного изъятия и/или саботажа(диверсии);
c) определение категорий ядерного материала и/или потенциальных последствий саботажа (диверсии), относящихся к каждой цели;
d) составление перечня целей для установки, включая описание каждой цели, которую необходимо защитить, указание ее категории и местонахождения. Перечень целей следует защищать как чувствительную информацию.

4.26. Рекомендуемые меры защиты для каждой категории ядерного материала описаны в [1], пункты 4.9–4.49.

4.27. При определении целей саботажа (диверсии) государству следует вначале установить пределы потенциальных радиологических последствий, которые оно решит отнести к неприемлемым радиологическим последствиям и серьезным радиологическим последствиям (см. пункты 3.91–3.101).

4.28. Пункт 5.4 публикации [1] гласит:

> «Для каждой *ядерной установки* следует проводить анализ, адекватность которого проверяется *компетентным органом*, с целью определения соответствующего данному количеству радиоактивного материала потенциала приводить к *неприемлемым радиологическим последствиям*, определяемым государством, при допущении, что акты *саботажа (диверсии)* будут успешно совершены в условиях отсутствия мер физической защиты или мер по смягчению последствий».

Такой анализ касается двух видов саботажа (диверсии), которые могут привести к неприемлемым радиологическим последствиям, а именно прямого и непрямого саботажа (диверсии), которые описаны в [14]. Прямой саботаж (диверсия) предполагает использование энергии от внешнего источника, такого как обычные взрывчатые вещества, для рассеяния ядерного или другого радиоактивного материала; при непрямом саботаже (диверсии) используется энергия процессов, происходящих внутри ядерных или других радиоактивных материалов (например, тепло деления или радиоактивного распада), например за счет повреждения систем охлаждения активной зоны реактора.

4.29. Следует проводить консервативный анализ для определения потенциальных радиологических последствий, которые может повлечь за собой полный выброс суммарного объема ядерного или другого радиоактивного материала на каждой идентифицированной цели саботажа (диверсии) на установке. В случае непрямого саботажа (диверсии) ядерного материала этот суммарный объем может включать в себя продукты деления, образовавшихся в результате ядерной цепной реакции.

4.30. На ядерных установках принято проводить детальный анализ ядерной безопасности с целью демонстрации безопасности их эксплуатации. Информация из документации по техническому обоснованию безопасности может быть полезной для определения конструкций, систем и элементов, которые необходимо защитить от саботажа (диверсии). Также важно проанализировать другие возможные причины отказов в результате злоумышленных действий.

4.31. Оцененные потенциальные радиологические последствия для целей саботажа (диверсии) в дальнейшем используются для определения требований по физической защите указанных целей следующим образом:

a) если потенциальные радиологические последствия превышают предел серьезных радиологических последствий, то следует выделить и поставить под защиту особо важные зоны;
b) если потенциальные радиологические последствия попадают в промежуток между предельными значениями неприемлемых радиологических последствий и серьезных радиологических последствий, то государство определяет дифференцированные требования по защите исходя из уровня потенциальных последствий;

c) если радиологические последствия ниже предела неприемлемых радиологических последствий, то специальные требования по обеспечению физической защиты могут не устанавливаться, но оператору все равно следует обеспечить охрану и контроль доступа к оборудованию и устройствам, связанным с ядерной безопасностью.

Определение угроз

4.32. В рамках определения целей и требований к системе физической защиты государством должна быть определена угроза для установки посредством оценки угроз либо разработки проектной угрозы. Необходимая информация должна быть предоставлена оператору, и он должен использовать эту информацию как основу для проектирования и оценки системы физической защиты.

ПРОЕКТИРОВАНИЕ И ОЦЕНКА СИСТЕМЫ ФИЗИЧЕСКОЙ ЗАЩИТЫ

4.33. После определения целей и требований к системе физической защиты (этап 1) оператору или заявителю становятся известны цели системы физической защиты: что именно необходимо защищать (цель), от чего (угроза) и насколько тщательно (требования). Следующий шаг (этап 2) — это разработка проекта новой системы или внесение изменений в проект существующей системы с целью предусмотреть меры физической защиты для обнаружения, задержки и реагирования на уровне, достаточном для достижения целей такой системы. После того как система физической защиты будет спроектирована или охарактеризована, ее следует проанализировать и оценить (этап 3) для того, чтобы она соответствовала требованиям физической защиты. Оценка должна базироваться на общей эффективности системы, которая определяется эффективностью совместного действия различных мер по обеспечению защиты.

Этап проектирования (этап 2)

Общие соображения в отношении проектирования

4.34. На этом этапе проектировщик определяет, каким образом лучше всего объединить меры физической защиты, такие как заграждения, камеры, датчики, процедуры, средства связи и силы реагирования, в такую систему физической защиты, которая соответствовала бы требованиям к защите. При этом принимаются во внимание вопросы ядерной безопасности и

эксплуатации, чтобы были достигнуты цели физической защиты и ядерной безопасности. Общая цель — гарантировать, что система физической защиты соответствует требованиям к защите благодаря надлежащему балансу между функциями обнаружения, задержки и реагирования.

4.35. На рис. 5 проиллюстрированы принципы проектирования и показана временная шкала, которая используется применительно к конкретной системе физической защиты для определения того, будут ли силы реагирования достаточно заблаговременно и гарантированно оповещены, чтобы сработать прежде, чем нарушитель выполнит все задачи, необходимые для совершения конкретного злоумышленного действия. На верхней шкале показана временная последовательность нападения нарушителя и возможности системы физической защиты распознать присутствие нарушителя по ходу его движения к цели. Время реагирования системы физической защиты показано на нижней шкале диаграммы: на ней отмеряется время от первого полученного сигнала (см. пункты 4.62–4.67) о действиях нарушителя (T_0) до момента, когда нарушитель может быть остановлен (T_I). На данной диаграмме обнаружение происходит достаточно рано для того, чтобы силы реагирования могли пресечь действия нарушителя до наступления момента T_C, когда нарушитель успешно завершил бы свое нападение.

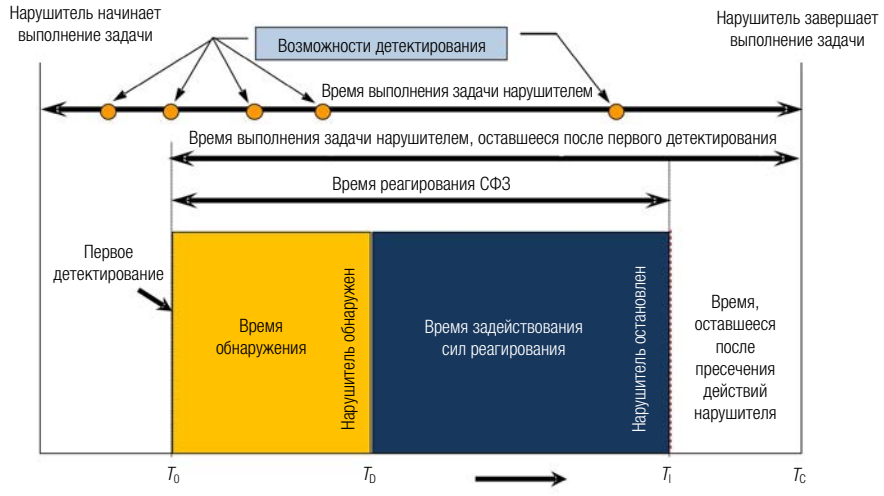

РИС. 5. Сравнение временных шкал действий нарушителя и сил реагирования. СФЗ — система физической защиты.

4.36. Положительная практика проектирования мер физической защиты предполагает обеспечение:

a) глубокоэшелонированной защиты, при которой нарушителю для успешного выполнения своей задачи необходимо обмануть, избежать или преодолеть несколько защитных заслонов по очереди. Глубокоэшелонированная защита обычно организуется путем размещения вокруг целей нескольких защитных заслонов, которые могут включать сочетание физических мер (например, контроль доступа в зоны, см. пункты 4.86–4.89) с административными (например, защита чувствительной информации и применение политики по проверке благонадежности персонала). Такой подход позволяет воспользоваться сильными сторонами каждого компонента физической защиты и использовать оборудование в сочетании, которое дополняет сильные стороны или компенсирует ограничения друг друга;
b) сбалансированной защиты, при которой нарушитель имеет дело с относительно эффективными мерами системы физической защиты независимо от того, когда, где и каким образом совершается злоумышленное действие;
c) надежности, означающей, что система физической защиты будет иметь высокую вероятность эффективного функционирования при самых разных типах действий нарушителя; надежность обычно достигается путем реализации в проекте принципов резервирования и неодинаковости.

4.37. Время, необходимо нарушителю для достижения поставленной цели, называется «временем выполнения задачи нарушителем» (см. рис. 5). Первостепенной функцией физических барьеров является увеличение времени выполнения задачи нарушителем путем создания препятствий на любом пути, который может выбрать нарушитель. Нарушитель должен быть вынужден проникнуть через несколько независимых барьеров или обойти их до того, как получит доступ к определенной цели. Время, которое требуется на проникновение или обход каждого из таких барьеров, необязательно должно быть одинаковым, но барьеры следует подобрать так, чтобы каждый требовал отдельного и несхожего с другими действия по мере продвижения нарушителя по своему пути. Эффект, который производит на нарушителя система физической защиты, спроектированная для обеспечения глубокоэшелонированной защиты, будет заключаться в том, чтобы:

a) повысить неуверенность нарушителя относительно устройства системы физической защиты;

b) потребовать от нарушителя дополнительных инструментов и более тщательной подготовки перед взломом системы физической защиты;
c) потребовать принятия дополнительных мер, которые могут привести к неудаче или заставить нарушителя отказаться от попытки нападения.

4.38. Надежность систем обнаружения и оценки можно обеспечить с помощью комбинации нескольких дополнительных датчиков и наблюдения персоналом. Для того чтобы дополнять друг друга, датчики на определенной границе или барьере выбираются таким образом, чтобы попытки обойти один датчик обнаруживались другими и разные датчики не реагировали на одни и те же источники ложных сигналов тревоги. Дополнительное выборочное или непрерывное наблюдение персоналом повысит неуверенность нарушителя относительно устройства системы физической защиты, что усложнит планирование и реализацию успешного нападения.

4.39. Проект системы физической защиты должен быть совместим с системами эксплуатации установки, важными с точки зрения безопасности, и давать возможность персоналу безопасно и уверенно выполнять свои обязанности. Если меры физической защиты усложнят персоналу выполнение его функций, персонал может найти пути обхода таких мер. Хорошее знание того, как функционирует ядерная установка, при проектировании системы физической защиты поможет найти баланс между потребностями физической защиты и потребностями ядерной безопасности и эксплуатации.

4.40. Подход к проектированию, описанный выше, был разработан и применяется для борьбы с внешними нарушителями. При проектировании системы физической защиты с целью противодействия инсайдерским угрозам необходимо учитывать дополнительные и/или другие факторы.

Дополнительные аспекты проектирования, касающиеся инсайдерских угроз

4.41. Внутренний нарушитель (инсайдер) определяется как одно или несколько лиц, имеющих официальный доступ к ядерным установкам или соответствующей чувствительной информации, которые могут совершить попытку несанкционированного изъятия или саботажа (диверсии) или содействовать внешнему нарушителю в совершении этого. Инсайдерская угроза — это намерение инсайдера совершить такое действие. Инсайдерами могут быть руководители, штатные работники, подрядчики

и работники сервисных служб, инспекторы и некоторые посетители. Таким образом, инсайдер может иметь любой статус на установке и может иметь официальный доступ в любую из контролируемых зон и к материалам.

4.42. Возможности инсайдера определяются тремя характеристиками:

a) уровень разрешенного доступа: в какие зоны установки инсайдер может или не может проникнуть при разных режимах работы установки (например, во время нормальной работы, в нерабочем состоянии, отключения для технического обслуживания) или во время событий, связанных с ядерной или физической ядерной безопасностью;
b) уровень полномочий по отношению к другим людям или определенным задачам и оборудованию;
c) знание целей, планировки установки, системы физической защиты и/или того, как заполучить и использовать специальные инструменты и оборудование, находящиеся на установке.

4.43. Инсайдерские угрозы представляют собой проблему, отличную от угроз внешнего нарушителя, потому что инсайдер может извлечь пользу из указанных характеристик для обхода некоторых технических и административных мер физической защиты с целью совершения или пособничества в совершении несанкционированного изъятия или саботажа (диверсии). Инсайдер также может внести свой вклад в злоумышленное действие посредством серии отдельных действий на протяжении длительного периода времени, что может снизить шансы на их обнаружение и, следовательно, повысить вероятность их успеха. Инсайдеры также могут иметь больше знаний и/или возможностей для выбора наиболее уязвимой цели и наилучшего времени для совершения злоумышленного действия.

4.44. Для защиты целей от злоумышленных действий с учетом проведенной государством оценки угроз или проектной угрозы проект системы физической защиты должен включать элементы, предотвращающие доступ несанкционированных лиц или оборудования к цели, а также сводящие к минимуму возможность совершения злоумышленного действия инсайдером, у которого есть такой доступ. Например, наличие барьеров в совокупности с эффективными силами реагирования может способствовать предотвращению доступа внешних нарушителей к цели, а ограничение доступа к оборудованию, связанному с целью, может обеспечить задержку даже инсайдеров, имеющих официальный доступ к зоне, где находится это оборудование, и может быть особенно эффективным, если такая зона находится под непрерывным наблюдением.

4.45. В [9] описан системный подход к защите от инсайдерских угроз, включая превентивные меры, сводящие к минимуму возможности инсайдера инициировать злоумышленное действие или содействовать ему, а также защитные меры с целью обнаружения, задержки, реагирования и смягчения последствий действия, совершенного инсайдером.

4.46. Защитные меры для противодействия инсайдерскому нападению начинаются с обнаружения нападения одним или несколькими имеющимися средствами, включая меры физической защиты, системы мониторинга технологического процесса, сигналы тревоги систем безопасности, сигналы тревоги системы учета и контроля ядерного материала на установке и наблюдение со стороны сотрудников и руководителей.

Этап оценки (этап 3)

> «3.29. *Оператору* следует разрабатывать и применять средства и процедуры проведения оценок, включая *проверку функционирования*, а также поддержания работоспособности *системы физической защиты*» [1].

4.47. На этапе 3 проводится оценка проекта системы физической защиты, разработанного на этапе 2 как для новой, так и для существующей системы, с целью определения того, соответствует ли проект требованиям, определенным на этапе 1. Причины, по которым осуществляется оценка системы физической защиты, могут состоять в следующем:

a) подтверждение того, что проект системы физической защиты или характеристики существующей системы физической защиты соответствуют требованиям физической защиты;
b) выявление любых недостатков в проекте или реализации проекта системы, которые необходимо учесть для выполнения требований к системе;
c) анализ потенциальных усовершенствований, которые могут требоваться для устранения выявленных недостатков и улучшения функционирования системы (включая усовершенствования, необходимые в связи с изменением угрозы);
d) повторная оценка эффективности системы физической защиты на ежегодной основе или через другие регулярные промежутки времени для учета всех изменений в целях или на установке.

4.48. Система физической защиты выполняет функции обнаружения, задержки и реагирования с помощью конструктивных, технических и кадровых элементов. Интеграция данных элементов с оборудованием и процедурами делает оценку эффективности системы физической защиты сложной задачей.

4.49. На этапе оценки собираются данные о функционировании мер в рамках системы физической защиты, которые используются для оценки общей эффективности системы физической защиты.

Оценка и проверка функционирования системы физической защиты оператором

4.50. В [1] акцентируется внимание на оценке и проверке функционирования системы физической защиты; в качестве примера можно привести нижеследующие положения.

a) Операторам следует «разрабатывать и применять средства и процедуры проведения оценок, включая *проверку функционирования*» ([1], пункт 3.29).
b) Для ядерных материалов категорий I и II: «Следует регулярно проводить оценки — включая *проверки функционирования — мер физической защиты* и *системы физической защиты*, в том числе своевременности реагирования *сотрудников охраны* и *сил реагирования*, с целью определения надежности и эффективности противодействия *угрозам*» ([1], пункт 4.35).
c) Для ядерных материалов категории I: «Как минимум один раз в год в проводимые *проверки функционирования системы физической защиты* следует включать соответствующие учения, например *двухсторонние учения...*» ([1], пункт 4.49).
d) Для саботажа (диверсии), который потенциально может повлечь серьезные радиологические последствия:

«Следует регулярно проводить оценки — включая *проверки функционирования — мер физической защиты* и *системы физической защиты*, в том числе своевременности реагирования *сотрудников охраны* и *сил реагирования*, с целью определения надежности и эффективности противодействия *угрозам*... В *проверки функционирования системы физической защиты* следует включать соответствующие учения, например *двухсторонние учения...*» ([1], пункт 5.41).

4.51. Эти положения подразумевают, что оператор должен планировать, проводить и документировать оценку и проверку функционирования системы физической защиты таким образом, чтобы соответствовать требованиям регулирующего органа. Соответствующие элементы этой оценки и проверки следует учитывать на протяжении всего жизненного цикла ядерной установки (т.е. во время проектирования, сооружения, лицензирования, эксплуатации, внесения изменений или усовершенствований, вывода из эксплуатации и обращения с радиоактивными отходами и отработавшим топливом).

4.52. Оператору следует рассмотреть возможность привлечения независимых экспертов для анализа результатов оценки и проверки функционирования системы в части, касающейся ядерных материалов категории I и саботажа (диверсии), который потенциально может привести к серьезным радиологическим последствиям.

Методы системной оценки

4.53. Существуют несколько подходов, ориентированных на достижение определенных показателей, для оценки эффективности системы физической защиты от действий инсайдеров и внешних нарушителей. Методы оценки, ориентированные на достижение определенных показателей, состоят в следующем.

a) Анализ путей действий нарушителя. Данный метод оценки предполагает построение временных шкал, таких как шкала, показанная на рис. 5, для различных реалистичных путей, которыми может воспользоваться нарушитель для достижения цели. На основе временной шкалы анализ устанавливает, есть ли гарантия того, что нападение будет обнаружено в момент, когда остается еще достаточно времени, необходимого нарушителю для выполнения своей задачи, для пресечения его действий силами реагирования. Обычно время выполнения задачи и время реагирования измеряются или оцениваются в количественном выражении, а уровень эффективности элементов обнаружения является вероятностной оценкой, основанной на проверках функционирования.
b) Математическое моделирование. Этот метод оценки предполагает компьютерное моделирование системы физической защиты и кабинетные учения, которые позволяют рассматривать эффективность плана физической безопасности и плана чрезвычайных мер как основ для реагирования в свете смоделированных решений нарушителя

и сил реагирования на установке. Данные инструменты обычно используются для оценки общего функционирования системы физической защиты в части обнаружения, пресечения действий и нейтрализации смоделированных нарушителей, и при этом принимаются во внимание все меры. Моделирование также может использоваться для изучения определенных аспектов, таких как эффективность действий сил реагирования по нейтрализации нарушителей (т.е. предотвращение совершения действия нарушителем после обнаружения и задержки).

c) Учения. Этот метод оценки принимает разные формы — от ограниченных занятий по определенным элементам системы физической защиты, таких как реагирование на тревожную сигнализацию, до двухсторонних учений, направленных на проверку эффективности всей системы физической защиты против смоделированного нападения нарушителя. Моделирование может не учесть важных практических аспектов реагирования и упустить из виду важные аспекты сценария нападения. Поэтому моделирование не может полностью заменить собой учения с участием персонала установки и сил реагирования на местах.

4.54. Моделирование и учения обычно проводятся как часть анализа сценариев, в рамках которого идентифицируются и подробно описываются разные постулируемые нападения («сценарии»), а затем они моделируются или используются как основа для учений, чтобы определить эффективность системы физической защиты в каждом из сценариев. Анализ сценариев обычно строится на анализе путей действий нарушителя за счет изучения конкретных методов, которыми может воспользоваться нарушитель для того, чтобы обойти датчики, барьеры и системы связи, либо чтобы отвлечь внимание или устранить часть сил реагирования. Сценарии обычно разрабатываются экспертами по указанным вопросам, а затем для количественного или качественного определения эффективности системы используются учения и/или моделирование. При анализе сценариев может использоваться информация о временных шкалах, разработанных во время анализа путей действий нарушителя.

4.55. Анализ сценариев может включать сценарии, связанные со сговором инсайдеров с внешними нарушителями, в той мере, в какой такие сценарии соответствуют проектной угрозе или оценке угроз. Оценки, касающиеся внешних угроз, включают рассмотрение характеристик нарушителя, таких как число нападающих, их оборудование (включая оружие и

взрывчатые вещества) и навыки, которые могут помочь им обойти систему физической защиты. Обычно в анализ путей действий нарушителя входит использование специализированных инструментов.

4.56. Эффективность системы может быть измерена количественно или качественно. Государству следует решить, какие подходы должны использоваться для разных типов целей, угроз и сценариев. Предлагается, чтобы требуемый уровень общей эффективности системы физической защиты определялся консервативно как нижний уровень количественной или качественной эффективности системы физической защиты, который при учете всех правдоподобных путей и сценариев действий нарушителя все же соответствует целям, поставленным регулирующим органом.

4.57. Существуют две основных группы сценариев, касающихся двух основных угроз: несанкционированного изъятия и саботажа (диверсии). При несанкционированном изъятии нарушителю необходимо получить доступ к местонахождению искомого материала, а затем переместить ядерный материал в некое место за пределами площадки. В случае ядерного материала категории I эффективной стратегией реагирования будет отказ в доступе к ядерному материалу или, если доступ получен, нейтрализация нарушителя до того, как ядерный материал покинет площадку. При саботаже (диверсии) нарушителю необходимо получить доступ к искомому материалу и/или к особо важным зонам, а затем непосредственно совершить акт диверсии в отношении материала или косвенным образом вызвать выброс радионуклидов посредством акта диверсии в отношении оборудования. В этом случае стратегией реагирования будет отказ в доступе к материалу или оборудованию как минимум на период времени, который может потребоваться для совершения акта саботажа (диверсии).

Дополнительные аспекты оценки, касающиеся инсайдерских угроз

4.58. Оценки должны включать анализ уязвимости системы физической защиты для инсайдерских угроз. Руководящие указания по проведению таких оценок приводятся в [9]. Для целей анализа инсайдерские угрозы можно подразделить на пассивные (например, только сбор чувствительной информации) или активные; если они активные, можно также указать, готовы ли внутренние нарушители применить силу против цели или человека. С учетом оценки угроз или проектной угрозы в оценке может допускаться возможность сговора инсайдера с другим инсайдером или внешним нарушителем.

4.59. Сценарии, в которых рассматривается последовательность действий инсайдера, можно использовать для определения эффективности защиты установки от инсайдерских угроз. Временная шкала действий нарушителя может быть пригодна только для оценки сценариев нападений инсайдера, предполагающих непрерывную серию действий, которую можно оценить так же, как и внешние угрозы. Временная шкала действий активного инсайдера может представлять собой непрерывную последовательность задач, аналогично временной шкале для внешнего нарушителя (см. рис. 5), либо прерывающуюся последовательность задач, часть которых могут быть существенно разнесены во времени и/или выполняться в разных местах. Примером сценария с непрерывной временной шкалой является внезапное хищение, при котором инсайдер совершает попытку хищения ядерного материала посредством непрерывной серии действий. Примером инсайдерского сценария с прерывающейся временной шкалой является долговременное хищение, при котором инсайдер пытается завладеть значительным количеством ядерного материала посредством серии отдельных хищений небольших объемов за несколько дней или недель.

КЛЮЧЕВЫЕ ФУНКЦИИ СИСТЕМЫ ФИЗИЧЕСКОЙ ЗАЩИТЫ

4.60. Система физической защиты соответствует требованиям физической защиты и достигает целей физической защиты благодаря сдерживанию и сочетанию функций обнаружения, задержки и реагирования. В [17] содержатся дополнительные, более детальные указания по этим ключевым функциям системы физической защиты.

Сдерживание

4.61. Сдерживание достигается, если потенциальные нарушители считают установку непривлекательной целью и решают не совершать нападение, поскольку считают вероятность успеха слишком низкой (или если потенциальные негативные последствия для них самих слишком высоки). Для более эффективного сдерживания оператор может использовать хорошо заметные меры защиты, такие как видимое присутствие сотрудников охраны, патрулирующих установку, яркое освещение ночью, решетки на окнах и барьеры для проезда транспортных средств. Сдерживание может способствовать снижению мотивации для нападения, но оценить эффективность сдерживания сложно, а то и вовсе невозможно. Более того, видимость мер физической защиты и персонала может сделать их более уязвимыми для действий нарушителя.

Обнаружение

4.62. В системе физической защиты обнаружение — это процесс, который начинается с выявления потенциально злоумышленного или иного несанкционированного действия либо присутствия нарушителя, и включения сигнала тревоги. Данный процесс завершается после оценки причины появления сигнала тревоги.

4.63. На рис. 6 показана последовательность событий, связанных с обнаружением, и из него следует, что обнаружение не является однократным, моментальным событием. Действия потенциального нарушителя считаются обнаруженными только после того, как будут выполнены все этапы последовательности. Информация, необходимая для точной оценки сигнала тревоги, включает следующие сведения: кто (или что) вызвал срабатывание сигнала тревоги, какое конкретно действие вызвало срабатывание сигнала тревоги, где указанное действие произошло и сколько человек могут быть к этому причастны. Первые три шага на рис. 6 — активация датчика, включение сигнала тревоги и регистрация сигнала тревоги — представляют собой «детектирование»; последнее событие, оценка причины срабатывания сигнала тревоги, завершает процесс обнаружения.

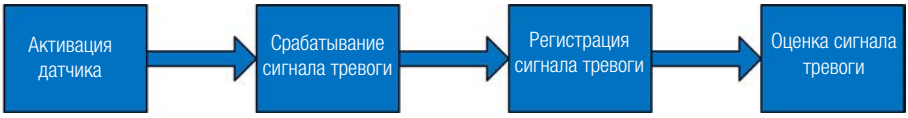

РИС. 6. Функция обнаружения в системе физической защиты.

4.64. Последовательность процесса обнаружения начинается в тот момент, когда какой-либо датчик активируется по любой причине. Активация датчика может означать срабатывание датчика аппаратуры (например, радиационного монитора или датчика движения) в системе физической защиты или донесение человека, например сотрудника охраны, о том, что он заметил нечто подозрительное.

4.65. Эффективное выполнение системой физической защиты функции обнаружения зависит от возможностей системы с точки зрения срабатывания датчиков, активации, регистрации и оценки сигнала тревоги, а также от работы персонала центральной станции тревожной сигнализации и всех сотрудников охраны сил и реагирования, которые

выполняют функции обнаружения. Эффективность на всех стадиях процесса обнаружения может быть повышена за счет использования технологий. В технологически оснащенной системе обнаружения должны использоваться датчики и системы видеонаблюдения, предоставляющие данные о детектировании и оценке действий нарушителя.

4.66. Эффективность обнаружения зависит как от вероятности обнаружения, так и от времени, которое требуется на выполнение процесса обнаружения. Вероятность обнаружения складывается из вероятности того, что действие будет засечено датчиками, что сигнал тревоги сработает и будет зарегистрирован и что причина срабатывания сигнала тревоги будет правильно оценена. Время обнаружения (с T_0 до T_D; см. рис. 5) — это совокупное время прохождения всех четырех этапов на рис. 6. Чем быстрее время обнаружения, тем более вероятно, что причина срабатывания сигнала тревоги будет оценена и сотрудники охраны вовремя прибудут на место для пресечения действий нарушителя, если это необходимо.

4.67. Обнаружение также может быть инициировано мерами контроля доступа, например в случае попытки несанкционированного проникновения на территорию людей, транспорта или запрещенных предметов, а также попытки несанкционированного изъятия ядерного материала.

Задержка

4.68. Задержка — это функция системы физической защиты, призванная замедлить продвижение нарушителя к цели и тем самым высвободить больше времени для эффективного реагирования. Задержка может обеспечиваться просто за счет расстояний и зон, которые требуется пересечь, и барьеров, которые необходимо преодолеть или обойти, такие как заграждения, ворота, порталы, двери, замки, решетки и активированные системы задержки. Барьеры могут остановить или нейтрализовать нарушителей, если они неспособны проникнуть через них. Каждый тип барьера требует у нарушителя времени на его преодоление или обход. Такое время задержки — фактор, который необходимо учитывать при проектировании системы физической защиты. Сотрудники охраны и силы реагирования могут обеспечить дополнительную задержку, если они надлежащим образом размещены, вооружены и защищены.

4.69. Важнейший критерий эффективности элемента задержки в системе физической защиты — это время, необходимое нарушителю после обнаружения для преодоления элемента, обеспечивающего задержку.

Никакая задержка, с которой сталкивается нарушитель до его обнаружения, не имеет значения для эффективности системы физической защиты по той причине, что такая задержка не дает дополнительного времени для реагирования на действия нарушителя. (Внешние барьеры также могут служить другим целям, таким как сдерживание или уменьшение последствий дистанционных нападений.) Задержка является особенно важной функцией в случаях, когда силы реагирования не базируются в непосредственной близости от установки и необходимо достаточное время задержки для того, чтобы они могли пресечь совершение злоумышленного действия.

Реагирование

4.70. Реагирование — это функция системы физической защиты, которая направлена на пресечение действий и нейтрализацию нарушителя до совершения злоумышленного действия. Сотрудникам охраны поручается контроль доступа, сопровождение лиц, отслеживание и оценка сигналов тревоги на центральной станции тревожной сигнализации, патрулированию и/или первоначальное реагирование при обнаружении потенциального нарушителя. Такие сотрудники охраны могут иметь или не иметь подготовки и полномочий для вооруженного реагирования. Силы реагирования состоят из находящихся на площадке или за ее пределами лиц, которые вооружены и надлежащим образом оснащены и подготовлены для пресечения и нейтрализации попыток несанкционированного изъятия или саботажа (диверсии) со стороны нарушителя.

ОБНАРУЖЕНИЕ И ВОЗВРАЩЕНИЕ ПРОПАВШИХ ИЛИ ПОХИЩЕННЫХ ЯДЕРНЫХ МАТЕРИАЛОВ

4.71. В зависимости от государственной правовой и регулирующей основы оператор обязан выполнить ряд шагов для содействия мерам по обнаружению и возвращению пропавшего или похищенного ядерного материала, подробно описанных в [1] следующим образом.

> «4.57. *Оператору* следует обеспечивать, чтобы любые пропавшие или похищенные *ядерные материалы* своевременно обнаруживались посредством таких систем, как *система учета и контроля ядерных материалов* и *система физической защиты* (например, путем

проведения периодических проверок инвентарного количества, инспекций, досмотров в пунктах контроля доступа, скрининга для обнаружения излучений).

4.58. *Оператору* следует подтверждать факт пропажи или похищения *ядерных материалов* путем оперативного проведения экстренной проверки инвентарного количества как можно скорее в пределах срока, установленного государством. Следует обеспечивать, чтобы *система учета и контроля ядерных материалов* позволяла получать точную информацию о возможно пропавших *ядерных материалах* на установке после возникновения *события, связанного с физической ядерной безопасностью*.

4.59. *Оператору* следует передавать сведения *компетентному органу* и другим соответствующим государственным организациям о пропавших или похищенных *ядерных материалах*, как это предписывается государством.

4.60. Меры, предпринимаемые *оператором* с целью определения места нахождения и возвращения пропавших или похищенных *ядерных материалов*, следует включать в принятый *оператором* к исполнению *план чрезвычайных мер* и регулярно проводить соответствующие проверки и оценки. Следует проводить надлежащие совместные учения (тренировки) с участием *компетентного органа* и других государственных организаций.

4.61. *Оператору* следует предпринимать все надлежащие меры для установления в кратчайшие сроки места нахождения любых *ядерных материалов*, заявленных пропавшими или похищенными, на площадке и возможно за пределами площадки (в случае преследования «по горячим следам») в соответствии с юридической и регулирующей системами и *планом чрезвычайных мер*.

4.62. Как можно скорее после установления места нахождения и идентификации пропавшего или похищенного *ядерного материала оператору* следует, в соответствии с *планом чрезвычайных мер*, обеспечить физическую безопасность этого материала на месте, а затем его возвращение на соответствующую *ядерную установку* после получения должного официального разрешения от *компетентного органа*.

4.63. *Оператору* следует оказывать государственным организациям любую иную необходимую помощь в целях определения места нахождения и возвращения *ядерных материалов* и сотрудничать во время проведения последующих расследований и в процессе судебного преследования».

4.72. Первым шагом в процессе обнаружения и возвращения пропавшего и/или похищенного ядерного материала является установление того, что ядерный материал не находится в положенном ему месте. Например:

a) система физической защиты может засечь попытку нарушителя похитить ядерный материал, и если система физической защиты не предотвратила такое действие, то ядерный материал может быть вынесен за пределы установки;
b) система учета и контроля ядерных материалов может обнаружить отсутствие ядерного материала во время эксплуатации, инвентаризации или инспекции;
c) досмотр в точках контроля доступа или скрининг излучений могут показать, что ядерный материал перемещается несанкционированным образом;
d) персонал установки может заметить и обнаружить, что кто-то пытается вынести ядерный материал.

4.73. После установления того, что ядерный материал не находится в положенном ему месте, оператору следует как можно скорее предпринять действия для подтверждения количества и типа(ов) пропавших ядерных материалов. После того как оператор подтвердит, что ядерный материал больше не находится в положенном ему месте, об этом следует оперативно уведомить соответствующие компетентные органы государства. В соответствии с планом чрезвычайных мер оператор может затем продолжить поиски такого материала в пределах площадки, а также при необходимости может инициировать поиски за пределами площадки в координации с соответствующими компетентными органами. В некоторых случаях такие поиски могут потребовать ввода в действие планов аварийных мероприятий [10, 12]. Зона, где ранее находился пропавший или похищенный материал, должна быть огорожена и рассматриваться как возможное место преступления. Следует также удостовериться, что остальному ядерному материалу по-прежнему обеспечивается физическая защита.

4.74. Все меры реагирования следует принимать в соответствии с планом чрезвычайных мер и согласовывать с соответствующими компетентными органами. После обнаружения ядерного материала оператору или другой соответствующей стороне следует обеспечить его охрану и возвращение в надлежащее место. Охрану и возвращение материала необходимо осуществлять в тесной консультации со всеми соответствующими компетентными органами, включая правоохранительные органы, особенно если уже начато или в ближайшее время будет начато уголовное расследование.

4.75. Механизмы координации операций и протоколов, связанных с возвращением ядерного материала, должны быть детально изложены в планах чрезвычайных мер и при необходимости согласованы с планами аварийных мероприятий. Предлагается, чтобы после любого инцидента с потерей материала проводилась последующая критическая оценка и чтобы уроки, извлеченные из реагирования, учитывались в новой редакции планов чрезвычайных мер.

СМЯГЧЕНИЕ ИЛИ СВЕДЕНИЕ К МИНИМУМУ РАДИОЛОГИЧЕСКИХ ПОСЛЕДСТВИЙ САБОТАЖА (ДИВЕРСИИ)

4.76. Реагирование на акт саботажа (диверсии) может требовать участия многих компетентных органов, в число которых могут входить компетентные органы, ответственные за реагирование на ядерную или радиологическую аварийную ситуацию, будь то в результате аварии или акта саботажа (диверсии). Для эффективного реагирования на акт саботажа (диверсии) такое реагирование следует должным образом интегрировать и координировать с реагированием на любую последующую аварийную ситуацию [10].

4.77. На оператора возлагаются нижеследующие обязанности по поддержке мер смягчения или сведения к минимуму радиологических последствий саботажа (диверсии), которые описаны в [1].

> «5.54. *Оператору* следует разрабатывать и применять *план чрезвычайных мер*.

5.55. *Оператору* следует осуществлять подготовку персонала установки, предусматривающую отработку действий в полной координации с *сотрудниками охраны*, *силами реагирования*, правоохранительными органами и группами реагирования на нарушение безопасности в целях осуществления *планов чрезвычайных мер*.

5.56. *Оператору* при *обнаружении злоумышленного действия* следует проводить оценку вероятности того, что данный акт может привести к радиологическим последствиям.

5.57. *Оператору* следует своевременно информировать *компетентный орган*, *силы реагирования* и другие соответствующие государственные организации об актах *саботажа (диверсиях)* или о попытках совершения *саботажа (диверсии)*, как это предписывается *планом чрезвычайных мер*.

5.58. Немедленно после обнаружения акта *саботажа (диверсии) оператору* следует принимать меры, направленные на предупреждение дальнейшего ущерба, обеспечение физической безопасности *ядерной установки* и защиту аварийного оборудования и персонала».

4.78. Все сотрудники сил реагирования на акт саботажа (диверсии) должны быть осведомлены об угрозах безопасности (например, о радиационном облучении), которые существуют внутри ядерной установки, и о том, как саботаж (диверсия) может повлиять на эти угрозы. Силы реагирования также должны соблюдать все соответствующие меры безопасности.

4.79. В планах чрезвычайных мер должны быть определены функции и обязанности всех соответствующих организаций, участвующих в реагировании на акт саботажа (диверсии), и содержаться, к примеру, следующие положения:

a) реагирование на площадке оперативно начинается и выполняется без ущерба для непрерывного осуществления функций эксплуатационной безопасности и физической защиты;
b) реагирование за пределами площадки эффективно выполняется и координируется с реагированием на площадке;
c) информация, необходимая для принятия решений относительно распределения ресурсов, оценивается на протяжении всего события.

4.80. Оператору следует включить в свой план чрезвычайных мер меры, которые направлены на предупреждение дальнейшего ущерба цели и другим частям установки, охрану ядерной установки и защиту аварийного оборудования и персонала.

4.81. Целью разработки и осуществления планов чрезвычайных мер является содействие ограничению последствий акта саботажа (диверсии). Реагирование на саботаж (диверсии) и реагирование на возникшую вследствие этого аварийную ситуацию может предполагать действия в одном и том же месте и в одно и то же время, но с разными целями. Следовательно, для обеспечения эффективности и совместимости планов чрезвычайных мер и планов аварийных мероприятий необходимо, чтобы они дополняли друг друга и совместно отрабатывались на регулярной основе. Необходимо проследить за тем, чтобы действия сил реагирования не оказывали негативного воздействия на ядерную безопасность и чтобы при осуществлении мер ядерной безопасности не страдала физическая защита. Пример плана чрезвычайных мер приведен в приложении II.

4.82. Служба аварийного реагирования, созданная для координации и организации реагирования на аварийную ситуацию на ядерной установке как на площадке, так и за пределами площадки независимо от того, какое событие вызвало аварийную ситуацию [10], может также использоваться для командования и управления функциями реагирования в рамках системы физической защиты.

МЕРЫ ФИЗИЧЕСКОЙ ЗАЩИТЫ

4.83. Система физической защиты, созданная на ядерной установке, должна соответствовать плану физической безопасности и детально в нем описываться. Такой план включает все аспекты мер физической защиты, определенные проектом системы физической защиты. Более подробная информация о применении мер физической защиты содержится в [17].

4.84. Меры физической защиты могут быть классифицированы по функциям, для которых они предназначены, о чем говорится в пунктах 4.60–4.70. В таблице 3 рекомендации разделов 4 и 5 публикации [1] для каждого типа мер физической защиты соотнесены с категорией ядерного материала для несанкционированного изъятия и с уровнем потенциальных последствий для саботажа (диверсии). В таблице также перечислены требования к оценке и проверке функционирования для каждого уровня защиты.

4.85. Рекомендации о мерах физической защиты в [1] выстроены на основе дифференцированного подхода. Меры, рекомендуемые для защиты ядерного материала категории II, также включают меры для категории III, а меры для защиты ядерного материала категории I также включают меры для категории II и категории III.

Зоны и уровни защиты

4.86. На рис. 7 показана основанная на рекомендациях пунктов 4.14, 4.22–4.28, 4.37–4.40, 4.42–4.46 и 5.20–5.35 публикации [1] концептуальная схема разных типов зон, которые организуются на ядерной установке в зависимости от ядерных материалов и целей саботажа (диверсии), для

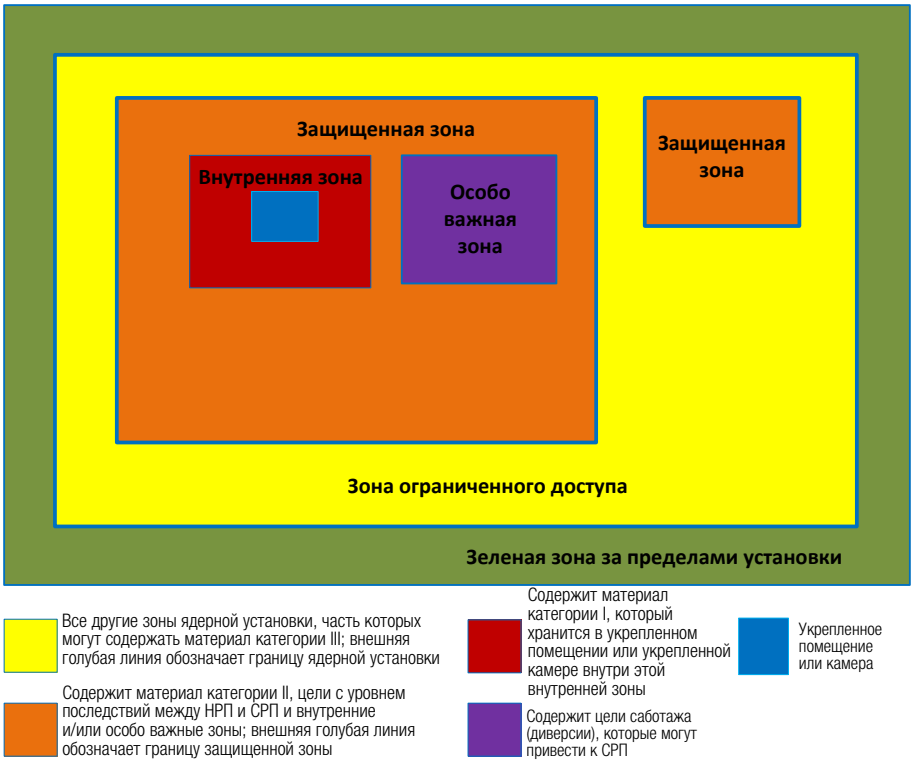

РИС. 7. План ядерной установки. НРП — неприемлемые радиологические последствия; СРП — серьезные радиологические последствия.

которых необходимо обеспечить глубокоэшелонированную защиту. Такие охраняемые зоны физически разделены в силу того, что у каждой зоны имеется собственный уровень защиты. Начиная с самой внутренней зоны, ниже описываются требования к уровню защиты каждой зоны с учетом рекомендаций о расположении зоны, доступе, обнаружении, задержке и реагировании.

Зона ограниченного доступа

4.87. Зона ограниченного доступа — это обозначенная зона, вмещающая ядерную установку и ядерный материал, доступ в которую ограничен и контролируется в целях обеспечения физической защиты. Любой ядерный материал категории III, находящийся в данной зоне, должен быть защищен путем применения мер, указанных в таблице 3. (Участок земли за границами ядерной установки также может быть контролируемой зоной в соответствии с национальной политикой.)

Защищенная зона

4.88. Ядерный материал категории II должен храниться в защищенной зоне. В соответствии с принципами дифференцированной защиты государство может рассмотреть возможность охраны целей саботажа (диверсии), потенциальные последствия которого варьируются от неприемлемых радиологических последствий до серьезных радиологических последствий, внутри защищенной зоны. Все защищенные зоны следует располагать внутри зоны ограниченного доступа и защищать посредством применения мер, указанных в таблице 3. Особо рекомендуется установка физических барьеров по периметру защищенной зоны.

Внутренние зоны и особо важные зоны

4.89. Внутренние зоны содержат ядерный материал категории I, а особо важные зоны содержат оборудование и/или радиоактивный материал, акт саботажа (диверсии) в отношении которого может привести к серьезным радиологическим последствиям. Внутренняя зона может также быть особо важной зоной; в таком случае следует применять меры как против несанкционированного изъятия, так и против саботажа (диверсии). Внутри внутренней зоны ядерный материал категории I должен храниться в укрепленном помещении или укрепленной камере. Все внутренние и особо важные зоны следует располагать внутри защищенной зоны и защищать посредством применения мер, указанных в таблице 3.

ТАБЛИЦА 3. МЕРЫ ФИЗИЧЕСКОЙ ЗАЩИТЫ УСТАНОВКИ: ПЕРЕКРЕСТНЫЕ ССЫЛКИ НА ПУНКТЫ ПУБЛИКАЦИИ [1]

	Несанкционированное изъятие ядерного материала при его использовании и хранении, по категориям материала			Саботаж (диверсия) на установках с серьезными последствиями	
	Категория III (зона ограниченного доступа)	Категория II (защищенная зона)	Категория I (внутренняя зона)	Защищенная зона	Особо важная зона
Меры физической защиты					
Обнаружение	4.14, 4.15, 4.16	4.14, 4.15, 4.16, 4.23, 4.30, 4.31	4.14, 4.15, 4.16, 4.23, 4.30, 4.31, 4.38, 4.40, 4.46, 4.47, 4.48	5.14, 5.21, 5.22, 5.36, 5.37	5.14, 5.26, 5.29, 5.33, 5.36, 5.37
Оценка сигнала тревоги	н.п.[a]	4.23, 4.30, 4.31	4.23, 4.30, 4.31, 4.47,	5.21, 5.36	5.36
Контроль доступа	4.14, 4.17	4.12, 4.17, 4.24, 4.25, 4.26, 4.27, 4.28, 4.30	4.12, 4.17, 4.24, 4.25, 4.26, 4.27, 4.28, 4.30, 4.38, 4.40, 4.42, 4.44, 4.45	5.14, 5.22, 5.23, 5.24, 5.25, 5.36	5.14, 5.26, 5.28, 5.31, 5.32, 5.34, 5.35, 5.36
Обнаружение запрещенных предметов	н.п.[a]	4.25	4.25, 4.43	5.14, 5.23	5.14
Центральная станция тревожной сигнализации	н.п.[a]	4.30, 4.31, 4.32, 4.33	4.30, 4.31, 4.32, 4.33, 4.47	5.36, 5.37, 5.38	5.36, 5.37, 5.38
Задержка	н.п.[a]	4.23	4.23, 4.38, 44.39, 4.41, 4.46	5.14, 5.21	5.14, 5.26, 5.27, 5.30
Реагирование	4.15, 4.19, 4.20	4.15, 4.19, 4.20, 4.30, 4.32, 4.33, 4.34	4.15, 4.19, 4.20, 4.30, 4.32, 4.33, 4.34, 4.49	5.14, 5.21, 5.36, 5.38, 5.39, 5.40, 5.42	5.14, 5.36, 5.38, 5.39, 5.40, 5.42
Оценка					
Проверка функционирования	4.20	4.20, 4.35	4.20, 4.35, 4.49	5.15, 5.16, 5.41	5.15, 5.16, 5.34, 5.41

[a] н.п: неприменимо.

Центральная станция тревожной сигнализации

4.90. Центральную станцию тревожной сигнализации рекомендуется оборудовать на всех ядерных установках, где хранятся ядерные материалы категории I и категории II и/или имеются цели саботажа (диверсии), потенциальные последствия которого превышают предел серьезных радиологических последствий.

4.91. К защите ядерных материалов категории I и категории II относятся следующие рекомендации:

> «4.30. Следует предусматривать создание *центральной станции тревожной сигнализации*, на которой постоянно должен находиться персонал для мониторинга и оценки тревожных сигналов, инициирования реагирования и связи с *сотрудниками охраны*, *силами реагирования* и руководством установки. Следует обеспечивать безопасное хранение информации, полученной на *центральной станции тревожной сигнализации*. *Центральную станцию тревожной сигнализации* следует, как правило, размещать в *защищенной зоне* и защищать так, чтобы она продолжала функционировать в условиях угрозы, например, путем укрепления соответствующего помещения. Следует строго ограничивать до минимума и контролировать доступ в помещение *центральной станции тревожной сигнализации*» [1].

4.92. Для целей саботажа (диверсии), потенциальные последствия которого превышают предел серьезных радиологических последствий, в [1] имеется рекомендация, которая, по существу, объединяет в себе рекомендации пунктов 4.30 и 4.47 данной публикации:

> «5.36. Следует предусматривать создание *центральной станции тревожной сигнализации*, на которой постоянно должен находиться персонал для мониторинга и оценки тревожных сигналов, инициирования реагирования и связи с *сотрудниками охраны*, *силами реагирования* и руководством установки. Следует обеспечивать безопасное хранение информации, полученной на *центральной станции тревожной сигнализации*. *Центральную станцию тревожной сигнализации* следует, как правило, размещать в *защищенной зоне* и защищать ее так, чтобы она продолжала функционировать в условиях угрозы, например, путем укрепления соответствующего помещения. Следует строго ограничивать до минимума и контролировать доступ в помещение *центральной станции тревожной сигнализации*. Следует предусматривать меры,

включая меры по резервированию, для обеспечения того, чтобы функции *центральной станции тревожной сигнализации* по мониторингу и оценке тревожных сигналов, инициированию реагирования и поддержанию связи сохранялись во время аварийной ситуации (например, посредством резервной станции тревожной сигнализации)» [1].

4.93. Главным компонентом центральной станции тревожной сигнализации является система аварийной сигнализации и оповещения. Такая система обеспечивает мониторинг и оценку тревожных сигналов на центральной станции тревожной сигнализации. Функции такой системы состоят как минимум в следующем:

a) передача тревожных сигналов и видеосигналов от датчиков и камер на центральную станцию тревожной сигнализации;
b) демонстрация такой информации оператору центральной станции тревожной сигнализации для использования в качестве основы для принятия решений и действий;
c) содействие оператору центральной станции тревожной сигнализации в оценке тревожных сигналов.

4.94. Положительной практикой является проектирование каналов передачи тревожных сигналов таким образом, чтобы они дублировались (т.е. две или более отдельных систем связи) и были неодинаковыми (например, отдельные системы используют разные физические каналы). Дублирование позволяет системе связи быть более надежной — если один канал связи выходит из строя, другие каналы могут взять на себя его функцию — и более защищенной, поскольку нарушителю потребуется обойти или вывести из строя как минимум два канала связи вместо одного.

4.95. В отношении защиты ядерных материалов категории I и категории II в [1] вынесены следующие рекомендации:

«4.31. Для оборудования тревожной сигнализации, каналов связи системы сигнализации и *центральной станции тревожной сигнализации* следует предусматривать источники бесперебойного питания и защиту от вмешательства в виде несанкционированного мониторинга, манипуляции и фальсификации.

4.32. Для осуществления деятельности, связанной с *обнаружением*, оценкой и реагированием, следует предусматривать специальные, резервированные, защищенные и неодинаковые системы передачи

сигналов с целью осуществления двусторонней речевой связи между *центральной станцией тревожной сигнализации* и *силами реагирования*. Следует обеспечивать специальную двустороннюю защищенную речевую связь между *сотрудниками охраны* и *центральной станцией тревожной сигнализации*».

Для целей саботажа (диверсии), потенциальные последствия которого превышают предел серьезных радиологических последствий, в [1], пункты 5.37 и 5.38, вынесены две аналогичные рекомендации.

4.96. Могут разрабатываться и применяться меры физической защиты для сохранения целостности системы аварийной сигнализации и оповещения во время события, связанного с физической ядерной безопасностью (они состоят в закрытии доступа к оборудованию и закрытии и обнаружении доступа к информации). Датчики индикации несанкционированного вскрытия кабельного ящика или аппаратного шкафа могут внести дополнительный вклад в физическую защиту.

4.97. Оператор центральной станции тревожной сигнализации несет ответственность за оценку тревожных сигналов и инициирование соответствующего реагирования на события, связанные с физической ядерной безопасностью. Ввиду этой важнейшей функции центральную станцию тревожной сигнализации обычно следует располагать внутри защищенной зоны. Поскольку центральная станция тревожной сигнализации является связующим звеном между функциями обнаружения и реагирования, операторам центральной станции тревожной сигнализации в идеале следует быть сотрудниками охраны и/или сил реагирования, так как они должны быть хорошо осведомлены о планах чрезвычайных мер и разбираться в них. Рекомендуется, чтобы функции центральной станции тревожной сигнализации регулярно отрабатывались во время нормальной эксплуатации и проверялись при более редких условиях эксплуатации.

4.98. Дополнительные рекомендации, касающиеся ядерных материалов категории I с потенциальными последствиями выше предела серьезных радиологических последствий, даны в [1], пункт 4.47:

«Следует предусматривать меры, включая меры по резервированию, для обеспечения того, чтобы функции *центральной станции тревожной сигнализации* по мониторингу и оценке тревожных

сигналов, инициированию реагирования и поддержанию связи сохранялись во время аварийной ситуации (например, посредством резервной станции тревожной сигнализации)».

Аналогичное положение в отношении целей саботажа (диверсии) с потенциальными последствиями выше предела серьезных радиологических последствий содержится в [1], пункт 5.36.

4.99. Ключевые функции центральной станции тревожной сигнализации при возникновении угрозы, сбое функционирования или эвакуации по причинам безопасности должны быть сохранены. В таких обстоятельствах бесперебойную работу ключевых функций центральной станции тревожной сигнализации может обеспечить резервная станция тревожной сигнализации. Такая резервная станция должна быть расположена отдельно от центральной станции тревожной сигнализации в месте, которое позволяет обеспечить бесперебойную работу ключевых функций центральной станции тревожной сигнализации. Системы физической защиты, располагающие как центральной, так и резервной станцией тревожной сигнализации, имеют следующие преимущества:

a) дублирование оборудования на двух станциях обеспечивает более высокую надежность аппаратуры;
b) центральная станция тревожной сигнализации может использоваться как основная система, наблюдение за работой которой может вестись с резервной станции;
c) резервная станция тревожной сигнализации может взять на себя функции управления системой физической защиты в случае отказа аппаратуры или проблем с персоналом на центральной станции тревожной сигнализации либо в случае нападения на центральную станцию тревожной сигнализации.

Физические барьеры

4.100. Физические барьеры следует размещать так, чтобы необходимость их преодолеть или обойти задержала нарушителя, а у сил реагирования появилось достаточно времени для пресечения действий нарушителя до того, как злоумышленное действие будет завершено. В сбалансированном проекте предусмотрено сбалансированное время задержки для разных путей движения нарушителя и сценариев, а физические барьеры тщательно планируются с учетом специфики места и располагаются на пути движения нарушителя. Величина времени задержки зависит от характера

установленных барьеров. В соответствии с оценкой угроз или проектной угрозой предлагается предусмотреть несколько уровней физических барьеров разных типов вдоль всех возможных путей движения нарушителя как способ усложнить и, следовательно, задержать продвижение нарушителя ввиду того, что нарушителю — помимо большего количества времени — потребуется использовать разнообразные инструменты и навыки. Чтобы облегчить оценку тревожных сигналов и дать возможность пресечь действия нарушителя в предсказуемых местах, физические барьеры и системы обнаружения следует устанавливать рядом друг с другом, так чтобы барьер оказался на пути нарушителя сразу после обнаружения нападения. Такая организация позволяет задержать нарушителя в точке обнаружения и повысить вероятность обнаружения нападения. Для обнаружения нападения или манипуляций с физическим барьером предлагается, чтобы барьеры, не защищенные системой обнаружения проникновения, осматривались в ходе выборочного патрулирования или обеспечивались другой формой наблюдения.

4.101. Транспортные средства могут с разгона прорваться через многие типы заграждений и закрытых ворот. В [1] рекомендовано, чтобы барьеры для транспортных средств устанавливались на надлежащем расстоянии от особо важных и внутренних зон. Для минимизации вероятности проникновения в любую охраняемую зону можно спроектировать и установить барьеры для транспортных средств в надлежащем месте на земле или воде. Расположение ворот для транспортных средств и подъезды к ним могут быть устроены таким образом, чтобы уменьшить вероятность прорыва через ворота транспортных средств с разгона. Подъездные дороги с несколькими резкими поворотами по обе стороны от ворот вынудят транспортные средства снизить скорость вблизи ворот, повысив тем самым эффективность барьеров для транспортных средств. Во всех случаях барьеры для транспортных средств должны проектироваться и использоваться таким образом, чтобы иметь возможность остановить транспортное средство, описанное в проектной угрозе или оценке угроз. Целесообразно установить надлежащую форму наблюдения за барьерами для транспортных средств с целью обнаружения манипуляций с ними.

Системы контроля доступа

4.102. Системы контроля доступа включают в себя оборудование, персонал и процедуры, используемые для подтверждения действительности пропусков и контроля движения людей и материалов в каждую зону и из каждой зоны. Системы контроля доступа используются для определения

того, кому разрешено войти, когда разрешено войти и где может быть произведен вход, а также для соблюдения требований пропускного режима. Информация, связанная с контролем доступа, является чувствительной и, следовательно, системы контроля доступа должны быть защищены соответствующим образом.

4.103. Системы контроля доступа можно спроектировать таким образом, чтобы они обеспечивали беспрепятственное и непрерывное передвижение в обе стороны санкционированных лиц, материалов и оборудования по стандартным маршрутам и в то же время обнаруживали и задерживали движение несанкционированных лиц и запрещенных предметов. Цели системы контроля доступа — разрешить передвижение в обе стороны только санкционированным лицам и транспортным средствам; обнаружить и предотвратить несанкционированное перемещение материала, информации или оборудования в зону или из зоны; дать информацию сотрудникам охраны для нужд оценки и реагирования; определить, что ведется учет людей во время события, связанного с физической ядерной безопасностью, или аварийной ситуации.

4.104. Системы контроля доступа в разные зоны на ядерной установке должны устанавливаться с учетом количества людей, которым требуется входить и выходить в каждой точке, и времени их входа и выхода. Поскольку система физической защиты имеет разные уровни защиты, в ней предусмотрены меры обнаружения разных типов и возрастающего уровня строгости на пути из зоны ограниченного доступа в защищенную зону и далее во внутренние и/или особо важные зоны. Число лиц, имеющих пропуска, будет все меньше на каждой последующей точке входа, и такой ограниченный доступ может повлиять на выбор оборудования и процедур для контроля доступа.

Сотрудники охраны и силы реагирования

4.105. Обязанности оператора по обеспечению реагирования в разных государствах неодинаковы, что обычно объясняется различиями в национальном законодательстве в части законного применения силы и прав ареста подозреваемых. В одних государствах оператор не несет главной ответственности за предоставление сил реагирования и такие силы предоставляются государством в соответствии с его нормативно-правовой базой. В некоторых других государствах оператор формирует как охранный контингент, так и силы реагирования из собственного штата сотрудников и/или подрядчиков. В подобных случаях оператор несет полную

ответственность за то, чтобы сотрудники охраны и силы реагирования на площадке, нанятые им в штат или на подрядной основе, выполняли свои соответствующие обязанности в соответствии с инструкциями руководства оператора и планом обеспечения физической безопасности.

4.106. Даже когда у оператора есть собственные сотрудники охраны и силы реагирования, силы реагирования за пределами площадки, подведомственные местным или национальным правоохранительным органам, также могут участвовать в реагировании, особенно в случае серьезного события, связанного с физической ядерной безопасностью. В таких случаях необходимо подписать договоренности между оператором и внешними организациями, предоставляющими силы реагирования; в таких договоренностях указываются цели, политика и концепция проведения операций по реагированию для всех сторон с целью гарантировать планомерное, скоординированное и эффективное реагирование. Такие письменные договоренности помогут обеспечить, чтобы план чрезвычайных мер оператора полностью соответствовал планам чрезвычайных мер внешних сил реагирования и был согласован с ними. Следует регулярно отрабатывать согласованные действия сотрудников охраны и сил реагирования в случае события, связанного с физической ядерной безопасностью. В случае ядерных материалов категории I и II и ядерных установок, саботаж (диверсия) на которых может привести к серьезным радиологическим последствиям, такая координация должна осуществляться на основе тесного взаимодействия между оператором и силами реагирования.

4.107. Кто бы ни отвечал за реагирование, силы реагирования должны быть способны пресечь действия и нейтрализовать нарушителя, у которого есть ресурсы и возможности, описанные в оценке угроз или проектной угрозе. Пресечение действий начинается с уведомления сил реагирования о том, что был обнаружен потенциальный нарушитель, и заканчивается, когда достаточное количество надлежащим образом обученных и оснащенных членов сил реагирования оперативно прибывает в надлежащее место для того, чтобы воспрепятствовать завершению злоумышленного действия нарушителем. Нейтрализация — это действие, следующее за пресечением и имеющее целью взять ситуацию под контроль прежде, чем цели нарушителя будут достигнуты, либо другим способом заставить нарушителей оставить свои попытки. Для эффективной нейтрализации силы реагирования должны превосходить нарушителей по численности, уровню оснащения и/или подготовки.

4.108. Эффективное информирование сил реагирования означает, что им предоставляется информация о действиях и характеристиках нарушителя (включая данные об их количестве по результатам наблюдения и любую имеющуюся информацию об инструментах, оборудовании, оружии и транспортных средствах) и даются инструкции по развертыванию сил реагирования. Эффективность информирования сил реагирования можно измерить вероятностью передачи точной информации и временем, необходимом для передачи точной информации силам реагирования.

4.109. Система физической защиты может включать в себя план обмена информацией для более эффективной координации действий по реагированию. Рекомендуется, чтобы система обмена информацией, используемая силами реагирования, давала возможность любому сотруднику сил реагирования скрытно отправить сигнал. Системы обмена информацией должны быть неодинаковыми и дублироваться для того, чтобы передача информации оставалась достаточно надежной для эффективного реагирования на угрозу, которая описана в проектной угрозе или оценке угроз.

4.110. Тщательно продуманная программа обучения — залог эффективного реагирования. Все сотрудники охраны, центральной станции тревожной сигнализации и сил реагирования должны участвовать в регулярных учебных занятиях, соответствующих их должности и функциям.

4.111. Рекомендации в [1] как для сотрудников охраны, так и для сил реагирования в случае события, связанного с физической ядерной безопасностью, состоят в следующем:

> «3.60. Следует регулярно проводить тренировки (учения) по отработке координации действий *сотрудников охраны* и *сил реагирования* в случае *события, связанного с физической ядерной безопасностью*. Кроме того, следует проводить тренировки и подготовку другого персонала установки, предусматривающие отработку действий в полной координации с *сотрудниками охраны*, *силами реагирования* и другими группами реагирования в целях выполнения имеющихся планов».

4.112. Конкретные рекомендации в [1] в отношении средств реагирования на несанкционированное изъятие ядерного материала категорий I, II и III состоят в следующем:

«4.15. Следует предусматривать меры для обнаружения несанкционированного проникновения и для осуществления соответствующих действий *сотрудниками охраны* и/или с*илами реагирования* достаточной численности в случае события, связанного с физической ядерной безопасностью.

…….

4.20. Государству следует обеспечивать, чтобы персонал *сил реагирования* был ознакомлен с площадкой и местами нахождения *ядерных материалов* и имел надлежащие знания вопросов радиационной защиты, с тем чтобы соответствующие подразделения были полностью готовы к осуществлению необходимых мер реагирования с учетом потенциальных последствий этих мер для безопасности».

4.113. Рекомендации в [1] по противодействию несанкционированному изъятию ядерного материала категорий I и II состоят в следующем:

«4.33. Следует предусматривать круглосуточную охрану и наличие *сил реагирования* для эффективного противодействия любым попыткам *несанкционированного изъятия*... Для *сотрудников охраны* и *сил реагирования* следует обеспечивать соответствующую подготовку и надлежащее оснащение, необходимые для выполнения ими своих функций в соответствии с национальным законодательством и регулирующими правилами.

4.34. Следует обеспечивать, чтобы *сотрудники охраны* проводили выборочное патрулирование *защищенной зоны*. Следует предусматривать, чтобы основными функциями патрулей были:

— сдерживание нарушителя;
— обнаружение проникновения;
— визуальный осмотр составных элементов физической защиты;
— дополнение существующих мер *физической защиты*;
— принятие первоначальных мер реагирования».

Рекомендация в [1], пункт 4.34, также применима к функциям сотрудников охраны внутри защищенных зон для защиты от саботажа (диверсии) (см. [1], пункт 5.40).

4.114. Положительной практикой является патрулирование всего периметра несколько раз за каждую смену, но в разное время, чтобы патрулирование было непредсказуемо для нарушителя, наблюдающего за установкой. Во время обхода патрули могут также проверить целостность заграждений, работу системы освещения и запорные устройства всех ворот и дверей. Другие положительные практики предполагают использование сотрудников охраны для тестирования работы датчиков по периметру защищенной зоны, проверки работоспособности системы обнаружения в других местах и принятия по мере необходимости компенсирующих мер, например до тех пор, пока неработающий датчик не будет отремонтирован или заменен.

4.115. В пунктах 3.27–3.32 и 4.50–4.52 содержатся рекомендации для государства и оператора, касающиеся соответственно оценки и проверки функционирования сил реагирования на несанкционированное изъятие ядерного материала категорий I и II и саботаж (диверсию).

4.116. Учения для сотрудников охраны и сил реагирования могут включать осуществление планов чрезвычайных мер, проверку функционирования, кабинетные учения, моделирование и имитацию, учения сил реагирования и/или двухсторонние учения.

Меры защиты от дистанционного акта саботажа (диверсии)

4.117. Оператор несет ответственность за защиту от тех типов дистанционных нападений, которые включены в проектную угрозу (см. пункты 3.55–3.63).

4.118. Первым шагом оператора в обеспечении защиты от дистанционных нападений является определение потенциальной уязвимости для дистанционного нападения зон, являющихся целью нападения, и материалов, оборудования и систем внутри таких зон. Данный процесс включает разработку сценариев саботажа (диверсии), основанных на определенных в оценке угроз или проектной угрозе характеристиках и на оценке поражения целей и системы физической защиты при таких сценариях. Этот процесс требует тесного взаимодействия между персоналом, ответственным за ядерную безопасность, и персоналом, ответственным за физическую защиту.

4.119. Оператор несет ответственность за проектирование мер защиты от дистанционных нападений и их применение после одобрения компетентным органом. Меры защиты, которые могут защитить от дистанционных нападений или смягчить их последствия, включают:

a) увеличение расстояния от установки, на которую может быть предпринято дистанционное нападение, чтобы такое расстояние превышало дальность действия оружия, которое может использовать нарушитель;
b) затруднение прямого обзора целей с мест, откуда может быть совершена попытка дистанционного нападения;
c) усиление функций обнаружения и сдерживания за счет патрулирования и наблюдения за пределами площадки;
d) использование барьеров, способных перехватить ракеты или принять на себя ударную волну или обломки от взрыва;
e) изменение планировки установок для защиты уязвимых целей;
f) укрепление установок для противодействия таким нападениям.

Меры защиты от нападений с воздуха и с воды

4.120. Оценка угроз или проектная угроза может включать нарушителей, использующих воздушное и/или водное транспортное средство в сценарии хищения или саботажа (диверсии) (не следует путать с дистанционным актом саботажа (диверсии) с воздуха). В таких случаях нарушители могут прибывать на место и/или покидать место по воде или воздуху. Оператор обычно несет некоторую ответственность за защиту установки от таких форм нападений.

4.121. Радиолокационные средства, акустические и сейсмические датчики могут дать некоторую возможность обнаружения нападений с воздуха, но они должны быть точно размещены для покрытия достаточно большой территории с минимальным количеством ложных сигналов тревоги. Можно не допустить посадки некоторых типов летательных аппаратов на площадке ядерной установки благодаря тому, что территория небольшая и/или плотно застроенная. Такой эффект может быть усилен за счет стратегического расположения столбов или других физических барьеров.

4.122. Оператор может установить и эксплуатировать оборудование и устройства для обнаружения таких нападений на основе проектной угрозы и требований государства.

Перевозка ядерного материала

4.123. Оператор ядерной установки как отправитель или получатель имеет определенные обязанности по обеспечению физической защиты ядерного материала, который ввозится на установку или вывозится с

нее. Эти обязанности могут включать предоставление предварительного уведомления о планируемой отправке груза, досмотр перевозочных средств, защиту конфиденциальной информации о перевозке, проверку целостности упаковки по прибытии и уведомление отправителя о таком прибытии, а также заключение предварительных договоренностей с перевозчиком о передаче ответственности за физическую защиту. Кроме того, оператору следует обеспечить, чтобы перемещение ядерного материала категорий I и II в пределах площадки между двумя защищенными зонами ядерной установки осуществлялось под охраной в соответствии с требованиями государства по перевозке ядерного материала за пределами установки. Дополнительные руководящие указания по обеспечению физической безопасности ядерного материала при перевозке содержатся в [2].

УЧЕТ И КОНТРОЛЬ ЯДЕРНЫХ МАТЕРИАЛОВ[4] ДЛЯ ЦЕЛЕЙ ФИЗИЧЕСКОЙ ЯДЕРНОЙ БЕЗОПАСНОСТИ

4.124. В [1] содержится ряд рекомендаций по учету и контролю ядерных материалов в части обеспечения физической ядерной безопасности:

> «3.26. *Оператору* следует постоянно обеспечивать контроль, а также ведение учета всех *ядерных материалов* на *ядерной установке*. Следует обеспечивать, чтобы оператор своевременно сообщал сведения о любом подтвержденном расхождении в учете, как это предусматривается *компетентным органом*.
>
> …….
>
> 3.36. При рассмотрении угрозы должное внимание следует уделять *внутренним нарушителям*. Последние могут пользоваться своими правами доступа, а также имеющимися у них полномочиями и знаниями для обхода специальных элементов физической защиты или других предусмотренных мер, таких как процедуры обеспечения безопасности. Следует обеспечивать, чтобы *система физической защиты* поддерживалась мерами по учету и контролю ядерных

[4] В английском тексте [1] используется термин «nuclear material accountancy and control»; в английском тексте [17] используется термин «nuclear material accounting and control». За исключением прямого цитирования [1], в настоящей публикации употребляется второй термин, но эти термины считаются взаимозаменяемыми.

материалов с целью сдерживания и обнаружения хищения *ядерного материала внутренним нарушителем*, совершаемого на протяжении длительного времени.

…….

3.47. При реализации принципа *глубокоэшелонированной защиты* следует учитывать способность *системы физической защиты* и *системы учета и контроля ядерных материалов* обеспечивать защиту от *внутренних нарушителей* и внешних угроз.

…….

4.57. *Оператору* следует обеспечивать, чтобы любые пропавшие или похищенные *ядерные материалы* своевременно обнаруживались посредством таких систем, как *система учета и контроля ядерных материалов* и *система физической защиты* (например, путем проведения периодических проверок инвентарного количества, инспекций, досмотров в пунктах контроля доступа, скрининга для обнаружения излучений).

4.58. *Оператору* следует подтверждать факт пропажи или похищения *ядерных материалов* путем оперативного проведения экстренной проверки инвентарного количества как можно скорее в пределах срока, установленного государством. Следует обеспечивать, чтобы *система учета и контроля ядерных материалов* позволяла получать точную информацию о возможно пропавших *ядерных материалах* на установке после возникновения *события, связанного с физической ядерной безопасностью*».

4.125. Система учета и контроля ядерных материалов создана для хранения информации о количестве, типе, местонахождении, использовании, перемещении и преобразованиях всего ядерного материала на установке. Функция учета ядерного материала обеспечивает сдерживание и обнаружение несанкционированного изъятия ядерного материала благодаря ведению инвентаризационного учета ядерного материала и его местоположения. Функция контроля ядерного материала обеспечивает меры по сохранению и наблюдению, позволяющие засечь злоумышленные действия инсайдера. Одна или обе эти функции могут обеспечить основу для инициирования реагирования, если будет обнаружено, что ядерный материал мог быть изъят без надлежащего разрешения или использован

несанкционированным образом. Эффективная система учета и контроля ядерных материалов повышает способность оператора обнаружить действия инсайдера и правильно оценить любые нештатные ситуации с ядерным материалом, инициированные инсайдерами или внешними нарушителями. Если ядерный материал перемещен с установки, система учета и контроля ядерных материалов должна быть способна определить количество и характеристики ядерного материала, который был перемещен.

4.126. Целями системы учета и контроля ядерных материалов в части обеспечения физической защиты являются:

a) обнаружение и оценка несанкционированного доступа к ядерному материалу или его изъятия;
b) предоставление информации о местонахождении, характеристиках и количестве ядерных материалов.

4.127. Достижение указанных целей позволит оператору:

a) сообщить соответствующим компетентным органам, что имело место несанкционированное изъятие ядерного материала;
b) предоставлять точную и своевременную информацию для содействия в обнаружении материала, который не находится в положенном ему месте;
c) обеспечивать, в координации с мерами физической защиты и контроля материала, гарантии того, что к ядерному материалу применяются надлежащие меры защиты и контроля в соответствии с его категорией.

4.128. Мониторинг и наблюдение за материалом могут использоваться оператором для обнаружения перемещения ядерного материала и непрерывного информирования о статусе оборудования учета и контроля ядерных материалов и самого ядерного материала. Мониторинг и наблюдение за материалом может включать визуальное наблюдение эксплуатационным персоналом и визуальный и удаленный мониторинг персоналом физической защиты, а также использование других технических средств, таких как датчики веса, датчики температуры, лазерные мониторы, радиочастотные маяки и датчики движения.

4.129. Для эффективного визуального наблюдения наблюдающий работник должен быть способен распознать несанкционированную деятельность, верно оценить ситуацию и своевременно доложить об этом соответствующему персоналу, отвечающему за реагирование,

для предотвращения несанкционированного изъятия. Если при таком наблюдении применяется правило «двух лиц», то два санкционированных лица должны пройти соответствующее обучение, иметь материал и друг друга в прямой видимости и быть способны обнаружить несанкционированные и некорректные процедуры.

4.130. Для обеспечения непрерывности поступления информации о ядерном материале и сигнализации о несанкционированном доступе могут использоваться меры по сохранению материала и устройства индикации несанкционированного вмешательства. Использование различных уровней сохранения — таких как контейнеры, перчаточные боксы, шкафы для хранения и камеры — вместе с эффективными устройствами индикации несанкционированного вмешательства и наблюдением сократит время, необходимое для определения пропажи материала и какого именно, а также того, требуется ли экстренная или внеплановая инвентаризация.

4.131. Положительной практикой считается распределение ответственности за отдельные функции учета ядерного материала, хранения ядерного материала и физической защиты между разными лицами или группами.

4.132. Своевременное обнаружение важно во всех случаях. Предлагается, чтобы оператор оценил все возможные меры обнаружения пропажи, хищения или другого несанкционированного перемещения ядерного материала, приблизительно рассчитав для каждого случая суммарное время обнаружения при помощи различных мер с целью определить, соответствует ли это требованиям, установленным компетентным органом. Дополнительные руководящие указания по данному вопросу содержатся в [18].

БЕЗОПАСНОСТЬ ЧУВСТВИТЕЛЬНОЙ ИНФОРМАЦИИ

4.133. Нарушители, которые хотят спланировать или совершить какое-либо злоумышленное действие в отношении ядерного материала или ядерной установки, могут с выгодой для себя использовать чувствительную информацию. Поэтому такую информацию следует идентифицировать, засекретить и защитить с помощью надлежащих мер.

4.134. Чувствительная информация — это информация в любой форме (включая программное обеспечение), несанкционированное раскрытие, корректировка, изменение, уничтожение или неиспользование которой могут поставить под угрозу физическую ядерную безопасность.

4.135. Пункт 1.2 публикации [16] гласит: «Конфиденциальность — такое свойство, при котором информация не предоставляется и не раскрывается лицам, организациям или процессам, не имеющим санкционированного доступа». Помимо защиты конфиденциальности чувствительной информации, информационная безопасность обеспечивает защиту точности и полноты информации (ее целостности) и доступности или удобства использования информации при необходимости (ее доступности).

4.136. Информационная безопасность — непременное условие физической ядерной безопасности во всех ее аспектах и один из ключевых элементов режима физической ядерной безопасности государства. Государство в лице компетентных органов устанавливает требования по информационной безопасности для операторов и других соответствующих организаций с учетом инструкций и правил органов национальной безопасности.

4.137. Оператор должен ввести внутренние правила и процедуры для защиты конфиденциальности, целостности и доступности чувствительной информации, которую оператор хранит или использует, в соответствии с политикой национальной безопасности и соответствующими национальными законами и требованиями. Такие процедуры должны быть инкорпорированы в план обеспечения физической безопасности. Оператор должен также обеспечить, чтобы его подрядчики, на площадке или за ее пределами, были поставлены в известность о чувствительности любой информации, передаваемой им оператором, и получили инструкции по процедурам надлежащей защиты такой информации. Оператор может нести ответственность за проведение проверок того, что подрядчики соблюдают эти процедуры, и обеспечение возвращения чувствительной информации оператору по окончании контракта.

4.138. Частые проверки и периодический аудит программы информационной безопасности могут использоваться для определения того, отвечает ли она своему назначению, и для ее улучшения или устранения любых выявленных недостатков. О случаях нарушения информационной безопасности следует сообщать в надлежащие органы для проведения расследований и принятия корректирующих мер в соответствии с требованиями государства.

4.139. Дополнительные руководящие указания по информационной безопасности, включая пример руководства по присвоению категорий секретности для содействия государствам и операторам в определении чувствительной информации, содержатся в [16].

ЗАЩИТА КОМПЬЮТЕРНЫХ СИСТЕМ

> «Компьютеризированные системы, используемые для обеспечения физической защиты, ядерной безопасности, а также учета и контроля ядерных материалов, следует защищать от компрометации (например, кибератак, манипуляции или фальсификации) в соответствии с *оценкой угроз* или *проектной угрозой*» ([1], пункты 4.10 и 5.19).

4.140. Государство несет ответственность за установление требований по компьютерной безопасности и обеспечение того, чтобы операторы гарантировали надлежащую защиту компьютеров и компьютерных систем от кибератак. Операторы несут ответственность за реализацию программы по обеспечению компьютерной безопасности в соответствии с такими требованиями.

4.141. Общей целью компьютерной безопасности в контексте физической защиты ядерного материала и ядерных установок является защита компьютерных систем от атак, направленных на то, чтобы облегчить несанкционированное изъятие ядерного материала или саботаж (диверсию). Оператор несет ответственность за определение компьютерных систем, которым необходима защита от компрометации, чтобы помочь предотвратить успешную атаку нарушителя. После этого оператор должен разработать политику компьютерной безопасности и план ее реализации.

4.142. Угрозы и атаки нарушителя могут быть разнонаправленными. Нарушителем может быть:

a) внешний нарушитель;
b) инсайдер;
c) одно или несколько лиц.

4.143. Атака может:

a) иметь немедленный эффект, вызвав повреждение оборудования или ослабление функций защиты;

b) быть длительной, такой как тайный сбор информации;
c) предполагать задержку, производя выдержанный по времени или независимо возникающий эффект;
d) быть синхронизированной с другими действиями нарушителя, которые могут включать физическое нападение.

4.144. Ниже перечисляются возможные типы атак.

a) Отказ в обслуживании или потеря функциональности. Данный тип атаки призван лишить оператора возможности отслеживать меняющиеся условия системы и/или реагировать на них путем замедления системы.
b) Перехват («незаконный посредник»). Такие атаки направлены на изменение входящей информации или сигналов команд для оборудования путем перехвата и изменения потоков данных между узлами компьютерной сети.
c) Скрытая система мониторинга и сбора информации. Несанкционированный доступ к файлам и запись информации, перехват сообщений (информации) и утечка информации могут дать необходимые данные для планирования и осуществления нападения.
d) Введение оператора в заблуждение, что приводит к некорректным действиям. Целью атаки является предоставление оператору ложных системных показателей посредством отправки потоков несанкционированных или ошибочных данных, что приводит к некорректным действиям оператора.
e) Прямые манипуляции с компьютерами и системами контроля. Нарушитель нацелен на получение независимого контроля над процессами и техникой.
f) Изменение эксплуатационных характеристик критически важных систем. За счет изменения логики системы, конфигурации оборудования, заданных значений или данных эти атаки ведут к изменению эксплуатационных характеристик системы, провоцируя аномальное поведение. Такое изменение критически важных систем может быть основной целью атаки либо средством для достижения других целей.

4.145. Защита от таких атак должна следовать подходу, основанному на принципе глубокоэшелонированной защиты, использующей технический и административный контроль, а также контроль физической безопасности. В этой связи компьютерная безопасность должна быть интегрирована в общую структуру плана обеспечения физической безопасности.

4.146. Детальные руководящие указания по разработке эффективной программы компьютерной безопасности на ядерных установках приводятся в [6].

ВЗАИМОДЕЙСТВИЕ МЕЖДУ БЕЗОПАСНОСТЬЮ И ФИЗИЧЕСКОЙ БЕЗОПАСНОСТЬЮ

> «4.11. *Оператору* следует проводить оценку взаимодействия физической защиты с мерами по обеспечению безопасности и учета и контроля ядерных материалов, а также управлять этим взаимодействием так, чтобы исключалось негативное влияние этих элементов друг на друга и чтобы в той степени, в которой это возможно, они взаимно дополняли друг друга» [1].

4.147. Эффективное управление взаимодействием между безопасностью и физической безопасностью — важный элемент обеих программ и залог обеспечения надлежащей физической защиты ядерного материала и ядерных установок и защиты здоровья и безопасности работников и населения.

4.148. Оператор несет основную ответственность за безопасность ядерной установки и меры физической защиты на данной установке. Операторам рекомендуется внедрить при помощи интегрированной системы менеджмента комплексный и скоординированный подход к рассмотрению предлагаемых изменений прежде, чем они будут внесены, для обеспечения того, чтобы изменения, предложенные по соображениям ядерной безопасности или физической защиты, не привели к непреднамеренному ухудшению ситуации в другой области. При выявлении потенциально неблагоприятного воздействия одной области на другую оператор должен поставить об этом в известность соответствующих работников организации и рассмотреть альтернативные меры либо принять компенсирующие меры и/или меры по смягчению последствий.

4.149. Оператор должен признать существующие проблемы взаимодействия между безопасностью и физической безопасностью и надлежащим образом решать их во время проектирования, сооружения и нормальной эксплуатации, а также во время событий, связанных с физической ядерной безопасностью, аварийных ситуаций и при выводе из эксплуатации. Эти проблемы могут решаться через действующие

механизмы управленческого контроля, такие как наблюдательные советы по безопасности и физической безопасности, планирование и контроль работ, а также управление конфигурацией.

4.150. Ниже приводятся примеры таких проблем во время событий, связанных с физической ядерной безопасностью, и аварийных ситуаций.

a) Координация реагирования по линии физической защиты на события, связанные с физической ядерной безопасностью, с реагированием по линии ядерной безопасности на любую аварийную ситуацию, возникшую в результате такого события.
b) Обеспечение того, что силы реагирования, обеспечивающие физическую защиту, были знакомы с ядерной установкой, включая местонахождение ядерного материала и оборудования/систем, важных для ядерной безопасности, и владели достаточными знаниями о требованиях радиационной защиты.
c) Обеспечение радиационной защиты сил реагирования при их проникновении в загрязненные зоны и прохождении через такие зоны во время акта саботажа (диверсии).
d) Защита сотрудников аварийно-спасательных служб ядерной безопасности и персонала установки, если им требуется войти в зоны или пройти через зоны, где работают силы реагирования во время события, связанного с физической ядерной безопасностью.
e) Обеспечение того, чтобы физические защитные барьеры отвечали целям физической защиты и не затрудняли действий персонала по организации быстрой эвакуации из зон в случае пожара, достижения критичности или выброса радионуклидов, например посредством установки встроенных быстро открывающихся замков на дверях и воротах в комбинации с сигналами тревоги. Могут потребоваться специальные физической защиты для быстрой эвакуации персонала из защищенной зоны в случае аварийной ситуации и одновременного досмотра персонала до выхода за территорию ядерной установки.
f) Установление требования о тщательной проверке и досмотре перед входом в защищенную зону без должного учета потенциальной необходимости быстрого проникновения в эту зону сотрудников и транспортных средств аварийного реагирования за пределами площадки для оказания помощи в случае медицинской или другой чрезвычайной ситуации.

4.151. Информация о взаимодействии между планами аварийных мероприятий и планами чрезвычайных мер представлена в пунктах 4.76–4.82, включая рекомендацию о совместной отработке действий в соответствии с обоими планами, которая улучшает их скоординированность.

4.152. Важным аспектом управления взаимодействием между безопасностью и физической безопасностью является информирование персонала, отвечающего за физическую защиту, об изменениях в физической планировке ядерной установки, конфигурации помещений, конструкций, систем и элементов, а также об изменениях в эксплуатации установки или аварийном планировании. Кроме того, целесообразно ознакомить компетентных сотрудников с изменениями в этих областях, прежде чем они будут внесены. Аналогичные процессы уведомления и рассмотрения полезны при анализе правил ядерной безопасности в свете изменений, связанных с мерами физической защиты. В частности, необходимы экспертные знания в области ядерной безопасности для рассмотрения любого нового определения предела неприемлемых радиологических последствий или изменения этих предельных значений с учетом изменений в эксплуатации или угрозах (которые затем лягут в основу решений об уровне физической защиты, который необходимо обеспечить для существующих и новых целей саботажа (диверсии)).

4.153. Эффективное управление взаимодействием между безопасностью и физической защитой означает применение мер безопасности и физической защиты таким образом, чтобы они дополняли друг друга. Например, процедуры ядерной безопасности, направленные на предотвращение инцидентов или аварий, могут также оказаться полезными при выполнении процедур физической защиты от злоумышленных действий инсайдера. Конструкции, системы и элементы, важные для ядерной безопасности, могут быть спроектированы и размещены на ядерной установке таким образом, чтобы упростить распределение обязанностей по защите целей саботажа (диверсии) и разделение ядерной установки на зоны с целью контроля доступа. Например, надлежащее физическое разделение оборудования ядерной безопасности в соответствии с принципом дублирования также уменьшает вероятность того, что все это оборудование будет повреждено в ходе одного акта саботажа (диверсии). Сокращение инвентарного количества ядерного материала и другие меры по уменьшению опасности снижает риски как для безопасности, так и для физической безопасности.

ПЛАН ОБЕСПЕЧЕНИЯ ФИЗИЧЕСКОЙ БЕЗОПАСНОСТИ

> «3.27. *Оператору* следует разрабатывать план обеспечения физической безопасности в рамках подачи заявки на получение лицензии. План обеспечения физической безопасности следует основывать на *оценке угроз* или *проектной угрозе*, и в него следует включать разделы по разработке, оценке, исполнению и поддержанию работоспособности *системы физической защиты*, а также *планы чрезвычайных мер*. *Компетентному органу* следует рассматривать и утверждать план обеспечения физической безопасности, осуществление которого должно затем стать частью условий лицензии. *Оператору* следует выполнять одобренный план обеспечения физической безопасности. *Оператору* следует регулярно рассматривать план обеспечения физической безопасности, обеспечивая, чтобы в него вносились изменения в соответствии с текущими условиями работы и действующей *системой физической защиты*. Перед внесением значительных изменений, включая временные изменения, в мероприятия, подробно изложенные в одобренном плане обеспечения физической безопасности, *оператору* следует представлять поправки к плану обеспечения физической безопасности для предварительного одобрения *компетентным органом*. *Компетентному органу* следует проверять соблюдение *оператором* плана обеспечения физической безопасности» [1].

4.154. План обеспечения физической безопасности — это один из основных элементов лицензирования ядерной установки государством, а применение плана обеспечения физической безопасности является условием выдачи лицензии для эксплуатации ядерной установки. Поэтому данный план должен в деталях описывать все аспекты системы физической защиты на ядерной установке. Рекомендуется включить в план обеспечения физической безопасности перечень целей на установке, указав для каждой цели, представляет ли она интерес с точки зрения несанкционированного изъятия и/или саботажа (диверсии). Рекомендуется также включить в план обеспечения физической безопасности меры физической защиты ядерного материала категорий I и II при его перемещении на площадке между двумя защищенными зонами, а также меры защиты ядерного материала при его получении на ядерной установке и отправке с установки.

4.155. В плане обеспечения физической безопасности описываются меры, принимаемые для достижения целей и соблюдения требований физической защиты государства. Таким образом, планы обеспечения физической безопасности должны основываться на подробном анализе и подкрепляться

достаточной информацией для подтверждения того, что все требования физической защиты при применении данного плана будут выполнены. План обеспечения физической безопасности дает гарантию реагирования системы физической защиты на угрозы, отраженные в оценке угроз или в проектной угрозе.

4.156. Пример структуры и предлагаемое содержание плана обеспечения физической безопасности представлены в приложении I.

Разработка, пересмотр и актуализация

4.157. Оператор должен постоянно обновлять план обеспечения физической безопасности, чтобы тот отражал существующие условия на ядерной установке, а также существующие угрозы. В этой связи в интегрированной системе менеджмента оператора должна иметься система управления физической безопасностью, обеспечивающая разработку, применение и контроль, а также актуализацию плана обеспечения физической безопасности и связанных с ним процедур. В процедурах применения могут быть описаны организационная структура физической безопасности, использование мер физической безопасности, таких как технологии и процедуры, обучение и квалификация персонала, отвечающего за физическую безопасность, и план чрезвычайных мер. При необходимости в плане обеспечения физической безопасности может быть приведен график выполнения отдельных частей плана и указаны любые действия, которые касаются модификации установки.

4.158. После одобрения компетентным органом план обеспечения физической безопасности включается в основу для лицензирования ядерной установки. Компетентный орган одобряет изменения в плане обеспечения физической безопасности, и оператору не разрешено вносить предложенные изменения в план обеспечения физической безопасности без одобрения компетентного органа за исключением случаев, когда такие изменения не снижают эффективность системы физической защиты. О незначительных изменениях, которые не снижают эффективность системы физической защиты, оператор должен в установленный срок уведомлять компетентный орган.

4.159. План обеспечения физической безопасности следует пересматривать с установленной компетентным органом периодичностью для того, чтобы он по-прежнему отражал текущие обстоятельства. План обеспечения физической безопасности также необходимо пересматривать

перед внесением изменений в штат, процедуры, оборудование или системы физической защиты, которые могут оказать негативное воздействие на физическую защиту. Введение новых количеств и типов ядерного материала, изменение целей саботажа (диверсии) и другие значительные изменения в системе физической защиты скорее всего потребуют изменений в плане обеспечения физической безопасности. Положительной практикой считается документирование и сохранение результатов такого пересмотра, в том числе всех составленных по его итогам планов действий.

Конфиденциальность чувствительной информации

4.160. Некоторая информация, содержащаяся в плане обеспечения физической безопасности, будет чувствительной, и ее несанкционированное раскрытие может нанести ущерб физической защите ядерной установки. Следовательно, оператору необходимо защищать план обеспечения физической безопасности от несанкционированного разглашения. В соответствии с требованиями государства доступ к чувствительной информации должен предоставляться только лицам, благонадежность которых была проверена и которым такая информация требуется для осуществления своих должностных обязанностей.

4.161. План обеспечения физической безопасности может быть разбит на разделы с разной степенью секретности, чтобы каждый раздел можно было при необходимости предоставлять лицам, которым требуется соответствующая информация и которые имеют надлежащий уровень благонадежности.

Приложение I

ПЛАН ОБЕСПЕЧЕНИЯ ФИЗИЧЕСКОЙ БЕЗОПАСНОСТИ

I.1. Пример возможной структуры плана обеспечения физической безопасности приведен во вставке 1. Далее вкратце описывается предлагаемое содержание каждого раздела. Государству и его компетентным органам следует рассмотреть предлагаемую структуру плана и модифицировать ее в соответствии со своими требованиями и конкретными нуждами.

ВСТАВКА 1. ПРИМЕРНАЯ СТРУКТУРА ПЛАНА ОБЕСПЕЧЕНИЯ ФИЗИЧЕСКОЙ БЕЗОПАСНОСТИ

1. АДМИНИСТРАТИВНАЯ ИНФОРМАЦИЯ

- 1.1. Введение и план реализации
- 1.2. Описание установки (эксплуатация и схема установки)
  - 1.2.1. Общее описание, назначение и эксплуатация установки
  - 1.2.2. Схема установки
- 1.3. Политика обеспечения физической безопасности
  - 1.3.1. Политика управления
  - 1.3.2. Культура физической ядерной безопасности
  - 1.3.3. Обеспечение качества
  - 1.3.4. Политика проверки благонадежности
  - 1.3.5. Программа обеспечения устойчивости
- 1.4. Организационное обеспечение физической безопасности
  - 1.4.1. Структура организационного обеспечения физической безопасности
  - 1.4.2. Управление безопасностью и распределение обязанностей
  - 1.4.3. Требование к квалификации персонала служб безопасности
  - 1.4.4. Обучение персонала служб безопасности
  - 1.4.5. Вооружение и снаряжение сотрудников охраны и сил реагирования
- 1.5. Защита ядерной информации
- 1.6. Компьютерная безопасность

ВСТАВКА 1: ПРИМЕРНАЯ СТРУКТУРА ПЛАНА ОБЕСПЕЧЕНИЯ ФИЗИЧЕСКОЙ БЕЗОПАСНОСТИ (продолжение)

2. ОПРЕДЕЛЕНИЕ СИСТЕМЫ ФИЗИЧЕСКОЙ ЗАЩИТЫ

- 2.1. Задачи системы физической защиты и требования к ней
- 2.2. Определение целей
- 2.3. Определение угроз
- 2.4. Взаимодействие с правоохранительными органами

3. СИСТЕМА ФИЗИЧЕСКОЙ ЗАЩИТЫ

- 3.1. Подробное описание системы физической защиты
- 3.2. Программа снижения инсайдерских угроз
- 3.3. Перевозка (транспортировка) ядерного материала
- 3.4. Испытания, оценка и техническое обслуживание системы физической защиты
  - 3.4.1. Типы испытаний и оценки
  - 3.4.2. Периодичность испытаний и оценки
  - 3.4.3. Техническое обслуживание
  - 3.4.4. Расширение и модернизация
- 3.5. Компенсирующие меры

4. ПЛАНИРОВАНИЕ РЕАГИРОВАНИЯ

- 4.1. Организация и обязанности
- 4.2. Службы безопасности
  - 4.2.1. Сотрудники охраны
  - 4.2.2. Силы реагирования на площадке
  - 4.2.3. Силы реагирования за пределами площадки
  - 4.2.4. Центральная станция тревожной сигнализации
- 4.3. План чрезвычайных мер
- 4.4. Командование и управление и каналы связи при инцидентах
- 4.5. Реагирование в условиях повышенной угрозы

5. ПРАВИЛА И РАБОЧИЕ ПРОЦЕДУРЫ

- 5.1. Документированные правила и рабочие процедуры
- 5.2. Рассмотрение, оценка, аудит и актуализация плана обеспечения физической безопасности
- 5.3. Оповещение об угрозах или инцидентах

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

СПИСОК СОКРАЩЕНИЙ И ГЛОССАРИЙ

I.2. Данный раздел содержит информацию о полном официальном наименовании и адресе организации, ответственной за защиту ядерной установки на основании закона. Соответствующие номера телефонов и факса и адреса электронной почты лиц, подающих заявку на одобрение плана обеспечения физической безопасности, могут содержаться в сопроводительном письме.

Введение и план реализации

I.3. Данный раздел включает краткое описание назначения и порядка эксплуатации установки, карты установки и другую информацию для обозначения на таких картах мест основной деятельности. На картах могут изображаться местность, транспортные маршруты, близлежащие города или предприятия с опасным материалом, а также любые другие объекты, которые могут повлиять на реагирование. На картах могут быть также обозначены основной и запасной маршруты для правоохранительных органов или других структур, осуществляющих реагирование за пределами площадки.

Описание установки (эксплуатация и схема установки)

I.4. В данном разделе содержатся подробные сведения о процессах эксплуатации ядерной установки.

Общее описание, назначение и эксплуатация установки

I.5. В данном разделе дается общее описание типов ядерной деятельности, которая ведется на установке, а также ядерного и другого радиоактивного материала, используемого или производимого в ходе такой деятельности.

Схема установки

I.6. В данном разделе может содержаться карта, схема или изображение установки с указанием ключевых зданий и видов деятельности. При описании деятельности установки могут использоваться блок-схемы различных процессов.

Политика обеспечения физической безопасности

I.7. В данном разделе излагается документированная политика обеспечения физической безопасности установки.

Политика управления

I.8. В данном разделе описывается система управления, обеспечивающая надзор за физической защитой установки, задачей которой является разработка, пересмотр, применение и контроль процедур обеспечения физической защиты. В данном разделе также может говориться о способах управления взаимодействием между безопасностью и физической защитой.

Культура физической ядерной безопасности

I.9. В данном разделе описывается, каким образом оператор способствует формированию культуры физической ядерной безопасности как важной части работы по донесению политики обеспечения физической безопасности до руководства, сотрудников и подрядчиков.

Обеспечение качества

I.10. В данном разделе описываются аспекты обеспечения качества в политике и программе управления, применимые к физической защите.

Политика проверки благонадежности

I.11. В данном разделе описываются уровни и требования благонадежности, применимые к работникам и подрядчикам на ядерной установке для предоставления доступа к определенным зонам внутри установки (например, защищенные зоны, внутренние зоны, особо важные зоны), ядерному материалу и чувствительной информации, а также меры для обеспечения постоянной благонадежности.

Программа обеспечения устойчивости

I.12. В данном разделе описывается программа обеспечения устойчивости системы физической защиты.

Организационное обеспечение физической безопасности

I.13. Для всех лиц, имеющих обязанности в области физической безопасности, может быть дано краткое описание их обязанностей и функций. Данный раздел может включать требования по отбору, обучению, оснащению, проверке и аттестации лиц, которые будут нести ответственность за защиту ядерного материала и ядерных установок. В соответствии с полномочиями и возможностями, предоставленными оператору, в нем должно определяться, какую часть функций по организации физической защиты обеспечивает персонал, а какую — внешние подрядчики. Что касается подрядчиков, то в данном разделе могут вкратце описываться письменные договоренности между оператором и подрядчиками, которые определяют, как подрядчики будут выполнять требования по физической защите установки. Уровень детализации плана обеспечения физической безопасности может варьироваться в зависимости от установки, но данный раздел должен содержать достаточную информацию для того, чтобы читатель уяснил возможности сил физической защиты установки. Предоставленная информация нацелена на подтверждение того, что система организации физической защиты разработана, укомплектована обученными и прошедшими аттестацию сотрудниками и оснащена оборудованием для обеспечения физической защиты.

Структура организационного обеспечения физической безопасности

I.14. В данном разделе описывается структура организационного обеспечения физической безопасности, включая руководство, сотрудников охраны и силы реагирования на площадке, технический персонал физической защиты и других лиц, ответственных за функции, связанные с физической защитой. Данный раздел также может содержать описание каждой руководящей и управленческой должности, включая круг обязанностей и полномочий вплоть до высшего руководства установки и организации.

Управление безопасностью и распределение обязанностей

I.15. В данном разделе описываются конкретные обязанности в области физической защиты, возложенные на организационную структуру установки.

Требования к квалификации персонала служб безопасности

I.16. Может быть дано описание начальных и последующих требований к квалификации лиц, которым поручаются функции и обязанности в области физической защиты. В данном разделе также может описываться процесс обеспечения того, чтобы такой персонал и в дальнейшем обладал необходимой квалификацией для оказания требуемых услуг. Данный раздел также включает описание требований по аттестации и переаттестации навыков владения огнестрельным оружием для сотрудников охраны и сил реагирования на площадке.

Обучение персонала служб безопасности

I.17. В данном разделе описывается программа обучения сотрудников охраны и сил реагирования на площадке. В нем также описывается, как они демонстрируют свое умение выполнять порученные им обязанности и функции. Для сил реагирования также может быть включено описание программы обучения по тактике реагирования.

Вооружение и снаряжение сотрудников охраны и сил реагирования

I.18. В данном разделе описывается оружие, которым оснащены сотрудники охраны и силы реагирования на площадке, в разбивке по должностям. Также может быть включено описание другого снаряжения, которым могут воспользоваться сотрудники охраны и силы реагирования для эффективного реагирования.

Защита ядерной информации

I.19. В данном разделе определены меры, которые принимаются для поддержания конфиденциальности, целостности и доступности чувствительной информации. В процедурах управления информацией также должен указываться, порядок передачи чувствительной информации только тем лицам, чья благонадежность была установлена надлежащим образом, на основе принципа служебной необходимости. Контроль, применяемый к чувствительной информации, может включать регистрацию ее приема, местонахождения, отправки и уничтожения.

Компьютерная безопасность

I.20. В данном разделе описываются действующие процедуры контроля доступа, протоколы и меры физической защиты для обеспечения конфиденциальности, целостности и доступности чувствительной информации, хранящейся на компьютерах и в компьютерных системах, а также целостности и доступности систем контроля и управления.

ОПРЕДЕЛЕНИЕ СИСТЕМЫ ФИЗИЧЕСКОЙ ЗАЩИТЫ

Задачи системы физической защиты и требования к ней

I.21. В данном разделе описаны задачи по защите целей различных типов, разбитых на группы исходя из их уровня чувствительности.

Определение целей

I.22. В данном разделе указаны потенциальные цели хищения или саботажа (диверсии) и их местонахождение. Он также содержит перечень компьютерных систем, важных для физической защиты, ядерной безопасности и учета и контроля ядерного материала, взлом которых может облегчить совершение злоумышленных действий.

Определение угроз

I.23. В данном разделе в общих чертах описаны типы угроз, защиту от которых призвана обеспечивать система физической защиты, и содержатся ссылки на оценку угроз или проектную угрозу, определенную государством.

Взаимодействие с правоохранительными органами

I.24. Может быть подробно описано, как поддерживается повседневное взаимодействие с правоохранительными органами для обеспечения раннего оповещения о потенциальных событиях, связанных с физической ядерной безопасностью.

СИСТЕМА ФИЗИЧЕСКОЙ ЗАЩИТЫ

I.25. В данном разделе содержится описание системы физической защиты на установке.

Подробное описание системы физической защиты

I.26. В данный раздел может быть включена карта установки с указанием границ охраняемых зон и мер защиты, таких как контрольно-пропускные пункты для персонала и транспортных средств. Необходимо дать описание мер физической защиты согласно приведенным ниже рекомендациям.

a) Контроль доступа. Необходимо описать порядок контроля и досмотра персонала, транспортных средств и материалов на каждом контрольно-пропускном пункте. Такое описание также может включать информацию о том, каким образом в пропускных системах и системах контроля доступа учтена необходимость быстрого перемещения через пункт имеющих на это право лиц и транспортных средств во время аварийных ситуаций или ситуаций, которые могут привести к аварийным. Можно уделить внимание вопросам контроля над всеми ключами, замками, комбинациями, паролями и соответствующими устройствами, необходимыми для пропуска в зоны ограниченного доступа, защищенные зоны, внутренние зоны, особо важные зоны и к оборудованию для обеспечения физической защиты.
b) Центральная станция тревожной сигнализации. В данном разделе указывается местонахождение центральной станции тревожной сигнализации и всех резервных станций мониторинга. В нем также описываются системы аварийной сигнализации и оповещения, аппаратура связи и порядок доступа на центральную станцию тревожной сигнализации, а также то, каким образом центральная станция тревожной сигнализации защищена от нападений и несанкционированного доступа.
c) Связь. Необходимо описать возможности связи, имеющиеся у сотрудников охраны и сил реагирования, а также механизмы связи между центральной станцией тревожной сигнализации, сотрудниками охраны и силами реагирования. В данном разделе описываются способы поддержания непрерывной связи для обеспечения эффективного командования и управления силами реагирования на площадке и за ее пределами как во время нормальных, так и во время аварийных ситуаций. Если на установке существуют зоны, где связь ограничена, эти зоны необходимо перечислить.

d) Обнаружение и наблюдение. В данном разделе описывается система обнаружения и способы передачи сигналов тревоги на центральную станцию тревожной сигнализации и их оценки. В нем также могут описываться процедуры действий в ситуациях, когда имеются признаки постороннего вмешательства. В нем описываются методы непрерывного обследования, наблюдения и мониторинга зон установки для обнаружения нарушителей и обеспечения целостности физических барьеров или других компонентов и функций системы физической защиты.

e) Освещение. В данном разделе описывается, как оператор поддерживает минимальный уровень освещения для решения определенных задач, таких как оценка после сигнала тревоги.

f) Физические барьеры. В данном разделе описываются барьеры в разных охраняемых зонах установки (например, здания, рельеф, заграждения, стены, двери). В нем также может содержаться описание барьеров для транспортных средств, их местонахождения и функционирования, а также соответствующие меры наблюдения.

g) Зоны/уровни безопасности. В данном разделе определяются зоны (или уровни) физической защиты, существующие на установке.

Программа снижения инсайдерских угроз

I.27. В данном разделе должны описываться меры защиты от инсайдерских угроз.

Перевозка (транспортировка) ядерного материала

I.28. В данном разделе описываются процедуры перевозки (транспортировки) разных категорий ядерного материала в пределах площадки, а также действующий на площадке порядок приема ядерного материала на установке и отправки ядерного материала с установки.

Испытания, оценка и техническое обслуживание системы физической защиты

I.29. В данном разделе определяются процедуры оценки и испытаний системы физической защиты.

Типы испытаний и оценки

I.30. В данном разделе описываются существующие программы испытаний и оценки и то, как они используются для оценки эффективности системы физической защиты установки.

Периодичность испытаний и оценки

I.31. Необходимо предоставить данные о периодичности, с которой проводятся программы испытаний и оценки.

Техническое обслуживание

I.32. В данном разделе описываются программы технического обслуживания и калибровки всего оборудования физической защиты.

Расширение и модернизация

I.33. Данный раздел подходит для описания предполагаемого графика работ по применению мер физической защиты, связанных с новым строительством или значительной физической модификацией существующих сооружений или установкой оборудования.

Компенсирующие меры

I.34. В данном разделе указываются все компенсирующие меры физической защиты, которые применяются, когда физические барьеры пришли в негодность или оборудование стало неработоспособным, в том числе в периоды плановых испытаний или технического обслуживания. В частности, следует описать порядок резервного электропитания всех типов оборудования физической защиты.

ПЛАНИРОВАНИЕ РЕАГИРОВАНИЯ

Организация и обязанности

I.35. В данном разделе содержатся сведения об организации и обязанностях сил реагирования на площадке и за ее пределами с целью обеспечить наличие эффективной стратегии реагирования для различных целей на установке.

Службы безопасности

I.36. В данном разделе описываются силы реагирования, которые могут участвовать в реализации скоординированной стратегии реагирования.

Сотрудники охраны

I.37. В данном разделе указывается количество, местонахождение и обязанности сотрудников охраны, включая данные об их вооружении, снаряжении и транспортных средствах.

Силы реагирования на площадке

I.38. В данном разделе описываются возможности сил реагирования на площадке и их способность оперативно отреагировать на события, связанные с физической ядерной безопасностью, если такие силы привлекаются.

Силы реагирования за пределами площадки

I.39. В данном разделе описываются возможности сил реагирования за пределами площадки и их способность отреагировать на события, связанные с физической ядерной безопасностью, включая предполагаемое время реагирования. Также можно включить информацию о процессе составления и исполнения соглашений об обеспечении реагирования за пределами площадки.

Подбор персонала для центральной станции тревожной сигнализации

I.40. В данном разделе указывается минимальное количество, обязанности, функции и график дежурств персонала, работающего на центральной станции тревожной сигнализации.

План чрезвычайных мер

I.41. В данном разделе описывается план чрезвычайных мер в случае событий, связанных с физической ядерной безопасностью, и других событий, которые могут потребовать реагирования служб физической защиты. В нем указываются конкретные лица, которые обязаны и уполномочены выполнять план чрезвычайных мер в случае события, связанного с физической ядерной безопасностью, и/или их должности. В нем указывается, как и когда план чрезвычайных мер пересматривается и отрабатывается.

I.42. Приведенный ниже список содержит примеры разных типов сценариев, которые могут учитываться и разбираться в плане чрезвычайных мер:

a) обнаружение и возвращение пропавшего ядерного материала (включая внеплановую инвентаризацию);
b) сведение к минимуму и смягчение радиологических последствий саботажа (диверсии);
c) обнаружение инсайдерской угрозы;
d) несанкционированное проникновение на ядерную установку;
e) внешние угрозы (например, предупреждение о закладке взрывного устройства);
f) дистанционное нападение;
g) нападение с воздуха;
h) нападение с воды;
i) кибератака;
j) разглашение чувствительной информации.

I.43. Поскольку план чрезвычайных мер будет содержать чувствительную информацию, он должен быть снабжен соответствующим грифом, указывающим требуемый уровень защиты. Также необходимо предусмотреть механизм координации плана чрезвычайных мер с планами аварийных мероприятий. Пример плана чрезвычайных мер приведен в приложении II.

Командование и управление и каналы связи при инцидентах

I.44. В плане обеспечения физической безопасности описывается, как будет осуществляться эффективное командование и управление организациями, привлеченными к реагированию на событие, связанное с физической ядерной безопасностью, где будет располагаться центр командования и управления при инциденте на площадке и за ее пределами и какие средства связи будут доступны в таких местах.

Реагирование в условиях повышенной угрозы

I.45. Необходимо включить перечень планируемых усовершенствований в процедурах физической защиты, которые будут внесены при любом возрастании общего уровня угрозы в государстве.

ПРАВИЛА И РАБОЧИЕ ПРОЦЕДУРЫ

Документированные правила и рабочие процедуры

I.46. В данном разделе перечисляются документированные правила и рабочие процедуры, регламентирующие физическую защиту на установке, включая процедуры взаимодействия с системами, которые дополняют систему физической защиты, такими как система ядерной безопасности и система учета и контроля ядерного материала.

Рассмотрение, оценка, аудит и актуализация плана обеспечения физической безопасности

I.47. Необходимо предоставить данные о процедурах и процессах рассмотрения (включая их периодичность), применяемых для того, чтобы сохранять актуальность плана обеспечения физической безопасности, а также гарантировать, что все необходимые поправки к нему будут перед внесением представляться на одобрение компетентному органу.

Оповещение об угрозах или инцидентах

I.48. В данном разделе описывается процедура, при помощи которой сотрудники и подрядчики установки могут оповещать о конкретных происшествиях организацию, отвечающую за физическую безопасность установки, а при необходимости в дальнейшем передавать такую информацию компетентному органу.

Приложение II

ПРИМЕР ПЛАНА ЧРЕЗВЫЧАЙНЫХ МЕР

ЦЕЛЬ

II.1. В данном разделе описывается цель конкретного плана чрезвычайных мер. Такой целью может быть подготовка к дальнейшему реагированию или смягчение последствий действий нарушителя.

ПРОЦЕДУРЫ РЕАГИРОВАНИЯ НА ИНЦИДЕНТЫ

Правила применения силы

II.2. В данном разделе описываются правила применения силы, которые определяют, какого рода силовое воздействие допускается законом и где и когда такое силовое воздействие может быть использовано.

Процедуры реагирования

II.3. В данном разделе описывается порядок организации и координации реагирования. В нем определяется, какие показатели будут использоваться, чтобы сигнализировать о начале реагирования в соответствии с планом чрезвычайных мер. Данный раздел может включать:

a) все заранее определенные действия, зоны ответственности и временные рамки для развертывания сил реагирования на сценарии хищения и саботажа (диверсии);
b) процедуры, которые ограничивают уязвимость сотрудников сил реагирования для возможного нападения;
c) временные рамки, используемые при уведомлении сил реагирования за пределами площадки;
d) минимальную численность сотрудников сил реагирования.

Обратный захват и возвращение

II.4. В данном разделе указывается, как организуется реагирование после того, как нарушитель покинул установку при сценарии хищения. Он включает протоколы, используемые для координации действий разных групп реагирования, систему подчинения и любые изменения в обязанностях.

Сведение к минимуму и смягчение последствий

II.5. В данном разделе указывается, как организуется реагирование службами физической защиты для помощи силам аварийного реагирования в сведении к минимуму и смягчении последствий акта саботажа (диверсии).

Командование и управление и каналы связи

II.6. В данном разделе описываются договоренности, закрепленные в протоколах с организациями, обеспечивающими внешнее реагирование. В нем указывается, какая служба руководит операцией и в каких ситуациях руководство может быть передано другой службе. Приводятся данные обо всех используемых каналах связи и о местонахождении центров управления при инцидентах, которые могут использоваться на разных этапах события с учетом сложившейся обстановки и стратегических и тактических функций центров.

ОТРАБОТКА ПЛАНА ЧРЕЗВЫЧАЙНЫХ МЕР

II.7. В данном разделе указываются типы и частота проведения учений для проверки и отработки действий в рамках плана чрезвычайных мер. Такая информация включает проверку согласованности между планом чрезвычайных мер и планом аварийных мероприятий посредством совместных учений, при которых применяются оба плана. В разделе также говорится о том, каким образом опыт, извлеченный из таких учений, документируется и используется для уточнения плана чрезвычайных мер.

Приложение III

СУММИРОВАНИЕ ИЛИ АГРЕГИРОВАНИЕ ЯДЕРНОГО МАТЕРИАЛА

ПОДХОД 1

III.1. Данный пример иллюстрирует один способ, которым можно использовать данные таблицы 1 для категоризации агрегированного ядерного материала. Ядерный материал, находящийся на одной и той же установке, разбивается на категории следующим образом:

a) Категория I, если:

$$\frac{\mathrm{Pu} + {}^{233}\mathrm{U}}{2000} + \frac{{}^{235}\mathrm{U}(\geq 20\%)}{5000} \geq 1 \tag{1}$$

b) Категория II, если:

$$\frac{\mathrm{Pu} + {}^{233}\mathrm{U}}{500} + \frac{{}^{235}\mathrm{U}(\geq 20\%)}{1000} + \frac{{}^{235}\mathrm{U}(\geq 10\% \text{ and } < 20\%)}{10000} \geq 1 > \frac{\mathrm{Pu} + {}^{233}\mathrm{U}}{2000} + \frac{{}^{235}\mathrm{U}(\geq 20\%)}{5000} \tag{2}$$

c) Категория III, если:

$$\frac{\mathrm{Pu} + {}^{233}\mathrm{U}}{15} + \frac{{}^{235}\mathrm{U}(\geq 20\%)}{15} + \frac{{}^{235}\mathrm{U}(\geq 10\% \text{ and } < 20\%)}{1000} + \frac{{}^{235}\mathrm{U}(> \mathrm{U}_{\mathrm{nat}} \text{ and } < 10\%)}{10000} \geq 1 > \frac{\mathrm{Pu} + {}^{233}\mathrm{U}}{500} + \frac{{}^{235}\mathrm{U}(\geq 20\%)}{1000} + \frac{{}^{235}\mathrm{U}(\geq 10\% \text{ and } < 20\%)}{10000} \tag{3}$$

d) Ниже категории III, если:

$$1 > \frac{\mathrm{Pu} + {}^{233}\mathrm{U}}{15} + \frac{{}^{235}\mathrm{U}(\geq 20\%)}{15} + \frac{{}^{235}\mathrm{U}(\geq 10\% \text{ and } < 20\%)}{1000} + \frac{{}^{235}\mathrm{U}(> \mathrm{U}_{\mathrm{nat}} \text{ and } < 10\%)}{10000} \tag{4}$$

или если материал состоит только из природного урана, обедненного урана и тория,

где

Pu	— масса в граммах всего плутония за исключением того, изотопный состав которого превышает 80% по ^{238}Pu;
^{233}U	— масса в граммах ^{233}U;
^{235}U (≥20%)	— масса в граммах ^{235}U, присутствующего в форме с обогащением по ^{235}U 20% или выше;
^{235}U (≥10% и <20%)	— масса в граммах ^{235}U, присутствующего в форме с обогащением по ^{235}U 10% или выше, но меньше 20%;
^{235}U (>Unat и <10%)	— масса в граммах ^{235}U, присутствующего в форме с обогащением по ^{235}U больше, чем природный уран, но меньше 10%;

и знаменателями дробей является масса в граммах.

III.2. Указанные формулы касаются материала, который не облучен в реакторе, или материала, который облучен в реакторе, но с уровнем излучения не более 1 Гр/ч (100 рад/ч) на расстоянии 1 м без защиты (биологической).

ПОДХОД 2

III.3. При другом подходе к определению категории агрегированного ядерного материала используется следующая формула:

$$\frac{1}{S} = \sum_i \frac{f_i}{S_i} \qquad (5)$$

где

fi (безразмерный)	— массовая доля материала типа *i в* смеси (масса каждого типа присутствующего материала, деленная на общую массу присутствующего материала);
Si (кг или г)	— предельное значение массы материала типа *i* для рассматриваемой категории, как указано в таблице 1;

и *S* (кг или г) — предельное значение массы агрегированного материала для рассматриваемой категории, как указано в таблице 1.

III.4. Предельные значения массы для категории I:

a) 2 кг плутония, включая все изотопы;
b) 5 кг ^{235}U в форме с обогащением по ^{235}U 20% или выше;
c) 2 кг ^{233}U.

III.5. Предельные значения массы для категории II:

a) 500 г плутония, включая все изотопы;
b) 1 кг ^{235}U в форме с обогащением по ^{235}U 20% или выше;
c) 10 кг ^{235}U в форме с обогащением по ^{235}U от 10%, но не более 20%;
d) 500 г ^{233}U.

III.6. Предельные значения массы для категории III:

a) 15 г плутония, включая все изотопы;
b) 15 г ^{235}U в форме с обогащением по ^{235}U 20% или выше;
c) 1 кг ^{235}U в форме с обогащением по ^{235}U от 10%, но не более 20%;
d) 10 кг ^{235}U в форме с обогащением по ^{235}U менее 10%;
e) 15 г ^{233}U.

III.7. Учитывается весь плутоний, за исключением плутония, изотопная концентрация которого по ^{238}Pu превышает 80%.

III.8. Эти предельные значения относятся к материалу, который не облучен в реакторе, или к материалу, который облучен в реакторе, но с уровнем излучения не более 1 Гр/ч (100 рад/ч) на расстоянии 1 м без защиты (биологической).

III.9. Для определение применимой категории вначале необходимо определить (шаг 1), относится ли агрегированный материал к категории I. Материал или смесь материалов относится к категории I, если агрегированная масса не менее предельного значения массы для категории I, рассчитанного для материала или смеси. Если материал или смесь не относится к категории I, то необходимо перейти к шагу 2.

III.10. Если агрегированный материал не относится к категории I, необходимо определить (шаг 2), относится ли он к категории II. Материал или смесь материалов относится к категории II, если агрегированная масса не менее предельного значения массы для категории II, рассчитанного для материала или смеси. Если материал или смесь не относится к категории II, то необходимо перейти к шагу 3.

III.11. Если агрегированный материал не относится к категории I или II, необходимо определить (шаг 3), относится ли он к категории III. Материал или смесь материалов относится к категории III, если агрегированная масса не менее предельного значения массы для категории III, рассчитанного для материала или смеси.

III.12. Если масса материала или смеси материалов меньше предельного значения для категории III, то он ниже категории III.

Пример 1

III.13. Ядерный материал состоит из 4 кг ^{235}U, содержащегося в уране, обогащенном свыше 20%, и 1 кг плутония, что в сумме составляет 5 кг ^{235}U и плутония. Массовая доля урана, обогащенного свыше 20%, составляет 4/5, плутония — 1/5.

Шаг 1. Предельное значение массы категории I для данного материала рассчитывается по следующей формуле:

$$\frac{1}{S} = \frac{4/5}{S_{\text{U-235}}} + \frac{1/5}{S_{\text{Pu}}} = \frac{4/5}{5\ \text{kg}} + \frac{1/5}{2\ \text{kg}} = 0.26$$

Следовательно, S = 3,85 кг. Поскольку масса материала (5 кг) больше, чем S (3,85 кг), она превышает предельное значение категории I для данной смеси.

Следовательно, материал соответствует количеству категории I.

Пример 2

III.14. Ядерный материал состоит из 2,5 кг ^{235}U, содержащегося в уране, обогащенного свыше 20%, и 500 г плутония, что в сумме составляет 3 кг ^{235}U и плутония. Массовая доля урана, обогащенного свыше 20%, составляет 2,5/3 (или 5/6), плутония — 0,5/3 (или 1/6).

Шаг 1. Предельное значение массы категории I для данного материала рассчитывается по следующей формуле:

$$\frac{1}{S} = \frac{5/6}{S_{\text{U-235}}} + \frac{1/6}{S_{\text{Pu}}} = \frac{5/6}{5\ \text{kg}} + \frac{1/6}{2\ \text{kg}} = 0.25$$

Следовательно, S = 4 кг. Общая масса равна 3 кг, что ниже предельного значения массы категории I для данной смеси.

III.15. Шаг 2. Предельное значение массы категории II для данного материала рассчитывается по следующей формуле:

$$\frac{1}{S} = \frac{5/6}{S_{\text{U-235}}} + \frac{1/6}{S_{\text{Pu}}} = \frac{5/6}{1\ \text{kg}} + \frac{1/6}{0.5\ \text{kg}}$$

Следовательно, S = 0,86 кг. Общая масса равна 3 кг, что выше предельного значения массы категории II для данной смеси. Следовательно, данная смесь относится к категории II.

Приложение IV

ПЕРЕКРЕСТНЫЕ ССЫЛКИ НА РЕКОМЕНДАЦИИ

Таблица 4 содержит перекрестные ссылки между пунктами публикации [1] и соответствующими пунктами настоящей публикации.

ТАБЛИЦА 4. ПЕРЕКРЕСТНЫЕ ССЫЛКИ НА «РЕКОМЕНДАЦИИ» [1]

Пункт(ы) «Рекомендаций» [1]	Соответствующие пункты настоящей публикации
ВВЕДЕНИЕ	Раздел 1
Общие сведения (1.1–1.8)	
Цель (1.9–1.11)	
Область применения (1.12–1.18)	
Структура (1.19–1.24)	
ЦЕЛИ ГОСУДАРСТВЕННОГО РЕЖИМА ФИЗИЧЕСКОЙ ЗАЩИТЫ (2.1–2.3)	Раздел 2
ЭЛЕМЕНТЫ ГОСУДАРСТВЕННОГО РЕЖИМА ФИЗИЧЕСКОЙ ЗАЩИТЫ, ДЕЙСТВУЮЩЕГО В ОТНОШЕНИИ ЯДЕРНЫХ МАТЕРИАЛОВ И ЯДЕРНЫХ УСТАНОВОК	
Ответственность государства (3.1, 3.2)	3.5–3.7
Международные перевозки (3.3–3.7)	Описано в [2]
Распределение ответственности за обеспечение физической защиты (3.8)	3.8–3.11
Законодательная и регулирующая основа	
Законодательная и регулирующая основа (3.9–3.17)	3.12–3.32
Компетентный орган (3.18–3.22)	3.39–3.48
Ответственность обладателей лицензии (3.23–3.30)	3.49. 4.4–4.13, 4.154–4.161

ТАБЛИЦА 4. ПЕРЕКРЕСТНЫЕ ССЫЛКИ НА «РЕКОМЕНДАЦИИ» [1] (продолжение)

Пункт(ы) «Рекомендаций» [1]	Соответствующие пункты настоящей публикации
Международное сотрудничество и помощь (3.31–3.33)	3.50–3.54
Идентификация и оценка угроз (3.34–3.40)	3.55–3.63
Система и меры физической защиты, основанные на учете рисков	
Управление риском (3.41, 3.42)	3.64–3.103
Дифференцированный подход (3.43, 3.44)	3.70–3.101
Глубокоэшелонированная защита (3.45–3.47)	3.102, 3.103
Обеспечение устойчивости режима физической защиты	
Культура физической безопасности (3.48–3.51)	3.105, 3.106
Обеспечение качества (3.52)	3.107–3.110
Конфиденциальность (3.53–3.55)	3.111–3.115
Программа обеспечения устойчивости (3.56, 3.57)	3.119
Планирование мероприятий, готовность на случай событий, связанных с физической ядерной безопасностью, и реагирование на такие события (3.58–3.62)	3.120–3.126
ТРЕБОВАНИЯ К МЕРАМ ЗАЩИТЫ ОТ НЕСАНКЦИОНИРОВАННОГО ИЗЪЯТИЯ ЯДЕРНЫХ МАТЕРИАЛОВ ПРИ ИХ ИСПОЛЬЗОВАНИИ И ХРАНЕНИИ	4.4–4.14, 4.23–4.59, 4.71–4.75, 4.124–4.139
Общие положения	
Основание для особого внимания (4.1–4.4)	
Категоризация (4.5–4.8)	3.74–3.90
Требования по обеспечению физической защиты от несанкционированного изъятия при использовании и хранении	
Общие положения (4.9–4.12)	4.83–4.123, 4.133–4.146

ТАБЛИЦА 4. ПЕРЕКРЕСТНЫЕ ССЫЛКИ НА «РЕКОМЕНДАЦИИ» [1] (продолжение)

Пункт(ы) «Рекомендаций» [1]	Соответствующие пункты настоящей публикации
Требования, применяемые в отношении ядерных материалов категорий I, II и III (4.13–4.20)	4.33–4.59, 4.83–4.123
Требования, применяемые в отношении ядерных материалов категорий I и II (4.21–4.35)	4.33–4.59, 4.83–4.123
Требования, применяемые в отношении ядерных материалов категории I (4.36–4.49)	4.33–4.59, 4.83–4.123
Требования к мерам по определению места нахождения и возвращению пропавших или похищенных ядерных материалов	4.71–4.75
Требования, применяемые в отношении государства (4.50–4.56)	
Требования, применяемые в отношении оператора (4.57–4.63)	
ТРЕБОВАНИЯ К МЕРАМ ЗАЩИТЫ ОТ САБОТАЖА (ДИВЕРСИИ), ПРИМЕНЯЕМЫМ В ОТНОШЕНИИ ЯДЕРНЫХ УСТАНОВОК И ЯДЕРНЫХ МАТЕРИАЛОВ ПРИ ИХ ИСПОЛЬЗОВАНИИ И ХРАНЕНИИ	4.4–4.14, 4.23–4.59, 4.76–4.82, 4.133–4.146
Общие положения (5.1–5.3)	
Основа для дифференцированного подхода к обеспечению физической защиты от саботажа (диверсии) (5.4–5.8)	3.91–3.101
Требования к процессу разработки системы физической защиты от саботажа (диверсий) (5.9–5.19)	4.140–4.153
Требования к обеспечению физической защиты от саботажа (диверсии) на ядерных установках	4.33–4.59, 4.83–4.123
Требования, применяемые в отношении установок, являющихся потенциальным источником серьезных последствий, включая атомные электростанции (5.20–5.42)	4.33–4.59, 4.83–4.123
Требования, применяемые в отношении других ядерных установок и ядерных материалов (5.43)	5.20–5.42

ТАБЛИЦА 4. ПЕРЕКРЕСТНЫЕ ССЫЛКИ НА «РЕКОМЕНДАЦИИ» [1] (продолжение)

Пункт(ы) «Рекомендаций» [1]	Соответствующие пункты настоящей публикации
Требования к сопутствующим мерам по смягчению или сведению к минимуму радиологических последствий саботажа (диверсии)	4.76–4.82
Рамки и сфера охвата (5.44)	
Требования, применяемые в отношении государства (5.45–5.53)	
Требования, применяемые в отношении оператора (5.54–5.58)	

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

[1] 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).

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

[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] 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).

[5] INTERNATIONAL ATOMIC ENERGY AGENCY, Establishing the Nuclear Security Infrastructure for a Nuclear Power Programme, IAEA Nuclear Security Series No. 19, IAEA, Vienna (2013).

[6] МЕЖДУНАРОДНОЕ АГЕНТСТВО ПО АТОМНОЙ ЭНЕРГИИ, Компьютерная безопасность на ядерных установках, Серия изданий МАГАТЭ по физической ядерной безопасности, № 17, МАГАТЭ, Вена (2012).

[7] ВСЕМИРНАЯ ТАМОЖЕННАЯ ОРГАНИЗАЦИЯ, ЕВРОПЕЙСКОЕ ПОЛИЦЕЙСКОЕ УПРАВЛЕНИЕ, МЕЖДУНАРОДНОЕ АГЕНТСТВО ПО АТОМНОЙ ЭНЕРГИИ, МЕЖДУНАРОДНАЯ ОРГАНИЗАЦИЯ ГРАЖДАНСКОЙ АВИАЦИИ, МЕЖДУНАРОДНАЯ ОРГАНИЗАЦИЯ УГОЛОВНОЙ ПОЛИЦИИ — ИНТЕРПОЛ, 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 по физической ядерной безопасности, № 15, МАГАТЭ, Вена (2011).

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

[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, МАГАТЭ, Вена (2009).

[10] 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).

[11] ПРОДОВОЛЬСТВЕННАЯ И СЕЛЬСКОХОЗЯЙСТВЕННАЯ ОРГАНИЗАЦИЯ ОБЪЕДИНЕННЫХ НАЦИЙ, МЕЖДУНАРОДНОЕ АГЕНТСТВО ПО АТОМНОЙ ЭНЕРГИИ, МЕЖДУНАРОДНАЯ ОРГАНИЗАЦИЯ ТРУДА, ПАНАМЕРИКАНСКАЯ ОРГАНИЗАЦИЯ ЗДРАВООХРАНЕНИЯ, ВСЕМИРНАЯ ОРГАНИЗАЦИЯ ЗДРАВООХРАНЕНИЯ, Критерии для использования при обеспечении готовности и реагирования в случае ядерной или радиологической аварийной ситуации, Серия норм безопасности МАГАТЭ, № GSG-2, МАГАТЭ, Вена (2012).

[12] ВСЕМИРНАЯ ОРГАНИЗАЦИЯ ЗДРАВООХРАНЕНИЯ, МЕЖДУНАРОДНОЕ АГЕНТСТВО ПО АТОМНОЙ ЭНЕРГИИ, МЕЖДУНАРОДНАЯ ОРГАНИЗАЦИЯ ТРУДА, 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] INTERNATIONAL ATOMIC ENERGY AGENCY, Identification of Vital Areas at Nuclear Facilities, IAEA Nuclear Security Series No. 16, IAEA, Vienna (2012).

[14] INTERNATIONAL ATOMIC ENERGY AGENCY, Engineering Safety Aspects of the Protection of Nuclear Power Plants against Sabotage, IAEA Nuclear Security Series No. 4, IAEA, Vienna (2007).

[15] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Culture, IAEA Nuclear Security Series No. 7, IAEA, Vienna (2008).

[16] INTERNATIONAL ATOMIC ENERGY AGENCY, Security of Nuclear Information, IAEA Nuclear Security Series No. 23-G, IAEA, Vienna (2015).

[17] INTERNATIONAL ATOMIC ENERGY AGENCY, Handbook on the Physical Protection of Nuclear Materials and Facilities, IAEA-TECDOC-1276, IAEA, Vienna (2002).

[18] INTERNATIONAL ATOMIC ENERGY AGENCY, Use of Nuclear Material Accounting and Control for Nuclear Security Purposes at Facilities, IAEA Nuclear Security Series No. 25-G, IAEA, Vienna (2015).

ЗАКАЗ В СТРАНАХ

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

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

СЕВЕРНАЯ АМЕРИКА

Bernan / Rowman & Littlefield
15250 NBN Way, Blue Ridge Summit, PA 17214, USA
Тел.: +1 800 462 6420 • Факс: +1 800 338 4550
Эл.почта: orders@rowman.com • Сайт: http://www.rowman.com/bernan

ОСТАЛЬНЫЕ СТРАНЫ

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

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

Торговые заказы и справочная информация:
Тел: +44 (0) 1767604972 • Факс: +44 (0) 1767601640
Эл.почта: eurospan@turpin-distribution.com

Индивидуальные заказы:
www.eurospanbookstore.com/iaea

Дополнительная информация:
Тел: +44 (0) 2072400856 • Факс: +44 (0) 2073790609
Эл.почта: info@eurospangroup.com • Сайт: www.eurospangroup.com

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

Группа маркетинга и сбыта (Marketing and Sales Unit)
Международное агентство по атомной энергии
Vienna International Centre, PO Box 100, 1400 Vienna, Austria
Телефон: +43 1 2600 22529 или 22530 • Факс: +43 1 26007 22529
Эл.почта: sales.publications@iaea.org • Сайт: https://www.iaea.org/ru/publikacii

Настоящая публикация — главное практическое руководство в комплекте руководящих документов по применению рекомендаций, содержащихся в публикации № 13 Серии изданий МАГАТЭ по физической ядерной безопасности «Рекомендации по физической ядерной безопасности, касающиеся физической защиты ядерных материалов и ядерных установок» (INFCIRC/225/Revision 5).

В руководстве рассматриваются вопросы физической защиты ядерного материала от несанкционированного изъятия и защиты ядерного материала и ядерных установок от саботажа (диверсии). В нем государствам и их компетентным органам даются рекомендации относительно создания, укрепления и поддержания национального режима физической защиты, а также применения связанных с ним систем и мер, в том числе систем физической защиты оператора.

МЕЖДУНАРОДНОЕ АГЕНТСТВО ПО АТОМНОЙ ЭНЕРГИИ
ВЕНА