Серия изданий МАГАТЭ по физической ядерной безопасности, № 8-G (Rev. 1)

Практическое руководство

ПРЕДУПРЕДИТЕЛЬНЫЕ И ЗАЩИТНЫЕ МЕРЫ, НАПРАВЛЕННЫЕ НА ПРОТИВОДЕЙСТВИЕ УГРОЗАМ, СОЗДАВАЕМЫМ ВНУТРЕННИМ НАРУШИТЕЛЕМ

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.

ПРЕДУПРЕДИТЕЛЬНЫЕ И ЗАЩИТНЫЕ МЕРЫ, НАПРАВЛЕННЫЕ НА ПРОТИВОДЕЙСТВИЕ УГРОЗАМ, СОЗДАВАЕМЫМ ВНУТРЕННИМ НАРУШИТЕЛЕМ

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, № 8-G (Rev. 1)

ПРЕДУПРЕДИТЕЛЬНЫЕ И ЗАЩИТНЫЕ МЕРЫ, НАПРАВЛЕННЫЕ НА ПРОТИВОДЕЙСТВИЕ УГРОЗАМ, СОЗДАВАЕМЫМ ВНУТРЕННИМ НАРУШИТЕЛЕМ

ПРАКТИЧЕСКОЕ РУКОВОДСТВО

МЕЖДУНАРОДНОЕ АГЕНТСТВО ПО АТОМНОЙ ЭНЕРГИИ
ВЕНА, 2023 год

УВЕДОМЛЕНИЕ ОБ АВТОРСКОМ ПРАВЕ

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

Отпечатано МАГАТЭ в Австрии
Февраль 2023 год
STI/PUB/1858

ПРЕДУПРЕДИТЕЛЬНЫЕ И ЗАЩИТНЫЕ МЕРЫ, НАПРАВЛЕННЫЕ НА ПРОТИВОДЕЙСТВИЕ УГРОЗАМ, СОЗДАВАЕМЫМ ВНУТРЕННИМ НАРУШИТЕЛЕМ
МАГАТЭ, ВЕНА, 2023 ГОД
STI/PUB/1858
ISBN 978–92–0–425521–8 (печатный формат) | ISBN 978–92–0–425621–5 (формат pdf)
ISSN 2788-8959

ПРЕДИСЛОВИЕ

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

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

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

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

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

РЕДАКЦИОННОЕ ПРИМЕЧАНИЕ

В настоящей публикации не затрагиваются вопросы ответственности — юридической или иного рода — за действия или бездействие со стороны какого-либо лица.

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 1

Общие сведения (1.1, 1.2) 1
Цель (1.3) 2
Область применения (1.4–1.7) 2
Структура (1.8) 3

2. ИДЕНТИФИКАЦИЯ УГРОЗ, СОЗДАВАЕМЫХ ВНУТРЕННИМ НАРУШИТЕЛЕМ (2.1, 2.2) 4

Атрибутивные признаки внутренних нарушителей (2.3–2.5) 4
Мотивация внутренних нарушителей (2.6–2.8) 6
Категории внутренних нарушителей (2.9–2.13) 7
Идентификация потенциальных угроз, создаваемых внутренним нарушителем (2.14–2.17) 8

3. ИДЕНТИФИКАЦИЯ ЦЕЛЕЙ (3.1, 3.2) 9

Цели для совершения несанкционированного изъятия (3.3–3.5) . . 10
Цели для совершения саботажа (3.6, 3.7) 11
Идентификация систем, используемых для обеспечения физической ядерной безопасности (3.8–3.11) 12

4. МЕРЫ, НАПРАВЛЕННЫЕ НА ПРОТИВОДЕЙСТВИЕ ПОТЕНЦИАЛЬНЫМ УГРОЗАМ, СОЗДАВАЕМЫМ ВНУТРЕННИМ НАРУШИТЕЛЕМ (4.1–4.3) 13

Общий подход к реализации (4.4–4.9) 14
Реализация мер, направленных на противодействие угрозам, создаваемым внутренним нарушителем (4.10–4.91) 15
Комплексные элементы, усиливающие предупредительные и защитные меры (4.92–4.102) 41

5. ОЦЕНКА МЕР 43

Цели и обзор процесса оценки (5.1–5.7) 43
Оценка предупредительных мер (5.8, 5.9) 45
Оценка защитных мер (5.10–5.17) 46

Оценка мер, направленных на противодействие сговору между внутренними нарушителями (5.18) 48
Оценка мер, направленных на противодействие хищению, совершаемому на протяжении длительного времени (5.19) 48
Оценка мер, направленных на противодействие саботажу (5.20–5.22) 49
Оценка установки на предмет обеспечения защиты от угроз, создаваемых внутренним нарушителем (5.23–5.27) 49

СПРАВОЧНЫЕ МАТЕРИАЛЫ 51

1. ВВЕДЕНИЕ

ОБЩИЕ СВЕДЕНИЯ

1.1. Серия изданий МАГАТЭ по физической ядерной безопасности содержит рекомендации для государств, помогающие им в реализации, рассмотрении и при необходимости укреплении национального режима физической ядерной безопасности. Данная серия также содержит руководства для государств по выполнению их обязательств, вытекающих из юридически обязывающих и не имеющих обязательной силы международных документов. В публикации «Основы физической ядерной безопасности» (Серия изданий МАГАТЭ по физической ядерной безопасности, № 20 [1]) изложены цель и основные элементы полного режима физической ядерной безопасности. В публикациях, содержащих рекомендации, указывается, что режим физической ядерной безопасности следует создавать для обеспечения физической защиты ядерного материала и ядерных установок [2], радиоактивного материала и связанных с ним установок [3], а также ядерного и другого радиоактивного материала, находящегося вне регулирующего контроля [4]. В этих публикациях, а также во многих других публикациях Серии изданий МАГАТЭ по физической ядерной безопасности [5–12] указаны конкретные угрозы, которые могут создаваться внутренними нарушителями, а также обращается внимание на необходимость принятия конкретных мер, направленных на противодействие угрозам, создаваемым внутренним нарушителем, и проведение соответствующей оценки этих мер.

1.2. Настоящая публикация представляет собой обновленное издание публикации в Серии изданий МАГАТЭ по физической ядерной безопасности, № 8, «Предупредительные и защитные меры в отношении угроз, исходящих от внутреннего нарушителя», опубликованной МАГАТЭ в 2008 году (в 2009 году на русском языке)[1]. Цели пересмотра сводились к тому, чтобы обеспечить большую согласованность настоящего Практического руководства с публикацией «Основы физической ядерной безопасности» и рекомендациями по физической ядерной безопасности, опубликованными после 2008 года, включить ссылки на другие практические руководства, опубликованные после 2008 года, а также добавить дополнительную

[1] 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).

детальную информацию по некоторым вопросам, учитывающую опыт МАГАТЭ и государств-членов, накопленный в использовании публикации Серии изданий МАГАТЭ по физической ядерной безопасности, № 8.

ЦЕЛЬ

1.3. В настоящем Практическом руководстве изложены обновленные рекомендации, предназначенные для государств, их компетентных органов и операторов[2], а также грузоотправителей и перевозчиков, по выбору, реализации и оценке мер, направленных на противодействие угрозам, создаваемым внутренними нарушителями (иногда называемыми «инсайдерами»). Угрозы ядерным установкам могут создаваться как внешними нарушителями, так и внутренними нарушителями или одновременно и теми и другими субъектами, действующими в сговоре (это может быть сговор о совместных действиях внутреннего нарушителя с другим внутренним или внешним нарушителем с намерением реализации незаконной или злоумышленной цели).

ОБЛАСТЬ ПРИМЕНЕНИЯ

1.4. Настоящая публикация посвящена вопросам применения предупредительных и защитных мер, направленных на противодействие несанкционированному изъятию ядерного материала и саботажу (диверсии), которые совершаются внутренними нарушителями в отношении ядерного материала и ядерных установок. Данное руководство применимо к любому типу ядерных установок, в частности, к атомным электростанциям, исследовательским реакторам и другим установкам ядерного топливного цикла (например, заводам по обогащению, заводам по переработке, заводам по изготовлению топлива, хранилищам), находящимся на стадиях проектирования, реконструкции, строительства, ввода в эксплуатацию, эксплуатации, остановки или вывода из эксплуатации.

---

[2] Термин «оператор» используется для описания субъекта (лица или организации), имеющего официальное разрешение на эксплуатацию ядерной или радиологической установки или официальное разрешение на использование, хранение или перевозку ядерного материала и/или радиоактивного материала. Как правило, такой субъект имеет лицензию или иное официальное разрешение, выданное компетентным органом, или является подрядчиком обладателя такого официального разрешения.

1.5. Руководящий материал, содержащийся в настоящей публикации по противодействию угрозам, создаваемым внутренним нарушителем, может также применяться для предотвращения и защиты от несанкционированного изъятия радиоактивного материала, а также актов саботажа (диверсии) в отношении радиоактивного материала и связанных с ним установок [3]; обеспечения физической безопасности ядерного и радиоактивного материала при транспортировании [6, 13], а также для предотвращения возникновения, обнаружения и реагирования в случае обнаружения ядерного и другого радиоактивного материала, находящегося вне регулирующего контроля [4]. Этот руководящий материал может также применяться в целях обеспечения защиты связанной с установкой информации, которой располагают или которую получили другие заинтересованные стороны, включая компетентный орган [8].

1.6. Для целей настоящей публикации доступ, который могут иметь внутренние нарушители на установке, включает физический доступ к определенным зонам и ядерному материалу, внутренний или разрешенный удаленный доступ к компьютеру или к компьютерной сети; доступ к чувствительной информации об установке.

1.7. Несмотря на то что вопросы ядерной безопасности не являются предметом настоящей публикации, следует обеспечивать, чтобы изложенные в ней предупредительные и защитные меры осуществлялись сбалансированным образом, совместимым с подходами, применяемыми в области обеспечения ядерной безопасности, а также с учетом требований в отношении обеспечения радиационной защиты работников. Меры по обеспечению физической ядерной безопасности и меры по обеспечению ядерной безопасности следует разрабатывать и осуществлять комплексно, добиваясь синергии между этими двумя сферами обеспечения безопасности, а также таким образом, чтобы меры по обеспечению физической ядерной безопасности не ставили под угрозу ядерную безопасность, а меры по обеспечению ядерной безопасности не осуществлялись в ущерб физической ядерной безопасности.

СТРУКТУРА

1.8. В настоящей публикации за введением следуют четыре раздела. Раздел 2 содержит информацию об угрозах, создаваемых внутренним нарушителем, и о категориях внутренних нарушителей. В разделе 3 дана информация об идентификации целей и систем установок, подлежащих

защите от злоумышленных действий со стороны внутренних нарушителей. Раздел 4 посвящен осуществляемым на уровне установки предупредительным и защитным мерам, направленным на противодействие угрозам, создаваемым внутренним нарушителем. В разделе 5 рассматривается оценка мер, изложенных в разделе 4.

2. ИДЕНТИФИКАЦИЯ УГРОЗ, СОЗДАВАЕМЫХ ВНУТРЕННИМ НАРУШИТЕЛЕМ

2.1. Термин «нарушитель» используется для описания любого лица, совершающего или пытающегося совершить злоумышленное действие. Нарушитель может быть внутренним или внешним.

2.2. Термин «внутренний нарушитель» (или также «инсайдер») означает:

> «Лицо имеющее официальный доступ к [ядерному материалу,] *соответствующим установкам или соответствующей деятельности*, либо к *чувствительной информации или активам чувствительной информации*, которое может совершить или содействовать совершению преступных или преднамеренных несанкционированных действий в отношении *ядерного материала*, *другого радиоактивного материала*, *соответствующих установок* или *соответствующей деятельности* или других действий, которые, согласно определению государства, могут негативно повлиять на физическую ядерную безопасность» [1].

Термин «внешний нарушитель» используется для обозначения нарушителя, не являющегося внутренним нарушителем.

АТРИБУТИВНЫЕ ПРИЗНАКИ ВНУТРЕННИХ НАРУШИТЕЛЕЙ

2.3. Внутренние нарушители характеризуются по меньшей мере одним из следующих атрибутивных признаков, обеспечивающих им преимущества

перед внешними нарушителями в случае попытки совершения злоумышленных действий:

a) доступ. Внутренние нарушители имеют санкционированный доступ к зонам, оборудованию и информации, необходимый им для выполнения служебных обязанностей. Он включает физический доступ на ядерную установку; к ядерным материалам и связанным с ними системам, элементам и оборудованию; к компьютерным системам установки. Доступ также включает удаленный компьютерный доступ к установке, такой как доступ к компьютерным системам и сетям, которые управляют процессами, обеспечивают безопасность, содержат чувствительную информацию или иным образом способствуют обеспечению физической ядерной безопасности. Оператор не должен разрешать удаленный доступ к критически важным системам, таким как системы, имеющие отношение к безопасности;
b) полномочия. Внутренние нарушители имеют право осуществлять операции в рамках возложенных на них обязанностей, а также могут иметь полномочия давать указания другим сотрудникам. Предоставленные полномочия могут использоваться в целях совершения злоумышленных действий, включая физические или совершаемые с помощью компьютера действия, такие как манипуляции с цифровыми файлами или процессами;
c) знания. Внутренние нарушители могут иметь в своем распоряжении знания об установке, о связанной с ней деятельности или о системах установки в объеме от ограниченных знаний до экспертного уровня. Благодаря этим знаниям внутренние нарушители могут иметь возможность действовать в обход или отключить специальные системы физической защиты и другие системы установки, используемые для обеспечения физической ядерной безопасности, такие как системы безопасности и системы учета и контроля ядерных материалов (СУиК ЯМ), эксплуатационные процедуры и функции реагирования.

Эти атрибутивные признаки могут также включать доступ к чувствительной информации или активам чувствительной информации или знаниям о них, включая информацию о транспортировании или перемещении ядерного материала [13].

2.4. Внутренний нарушитель может не характеризоваться всеми тремя атрибутивными признаками, однако при этом он может иметь достаточные возможности для совершения злоумышленного действия. Например, руководящий работник центрального аппарата может иметь ограниченный

физический доступ к установке, но в то же время может иметь право оформить заказ на доставку внешнему получателю по фальсифицированному адресу. Внутренние нарушители могут использовать поддельные полномочия или имеющиеся у них знания для содействия в совершении злоумышленного действия или для его инициирования. Внутренний нарушитель может действовать самостоятельно или в сговоре с другим внутренним или внешним нарушителем.

2.5. Благодаря имеющимся доступу, полномочиям и знаниям внутренние нарушители имеют возможность выбрать наиболее уязвимую цель и наилучшее время для попытки совершения или осуществления злоумышленного действия. Чтобы максимально повысить вероятность успеха, внутренний нарушитель может осуществлять план по совершению злоумышленного действия в течение продолжительного периода времени. Эта тактика может включать: a) вмешательство в оборудование, используемое для обеспечения физической защиты, или в оборудование, предназначенное для обеспечения ядерной безопасности, с целью подготовки к акту саботажа; b) фальсификацию учетных записей, позволяющую внутреннему нарушителю периодически осуществлять без обнаружения несанкционированное изъятие малых количеств ядерного материала более низкой категории, в отношении которого обеспечивается менее жесткая защита, чем в случае ядерного материала более высокой категории; c) несанкционированное изъятие ядерного материала в количествах ниже порогов обнаружения системы измерения. Внутренние нарушители могут иметь возможность совершить злоумышленное действие в нормальных или отклоняющихся от нормальных условиях на установке, в том числе во время проведения работ по техническому обслуживанию, или во время перемещения ядерного материала, и могут выбирать для этого наиболее подходящее время [14].

МОТИВАЦИЯ ВНУТРЕННИХ НАРУШИТЕЛЕЙ

2.6. Внутренние нарушители могут иметь разную мотивацию для совершения злоумышленных действий, включая деньги, идеологию, месть, эгоизм, принуждение или сочетание этих мотивов.

2.7. У внутреннего нарушителя может сформироваться собственная мотивация, достаточная для совершения злоумышленного действия, в частности по причине психического заболевания. Внутренний нарушитель

также может быть завербован внешним нарушителем, который планирует использовать доступ, полномочия или знания последнего. Внутреннего нарушителя могут склонить к совершению злоумышленного действия путем принуждения (например, шантажа).

2.8. Внутренний нарушитель может занимать любую должность в организации, от низшей до высшей категории. Внутренние нарушители на всех уровнях могут иметь достаточную мотивацию для совершения злоумышленного действия. Другой персонал, не нанятый непосредственно оператором, грузоотправителем или перевозчиком, но получающий санкционированный доступ на периодической основе к установке или ее системам (например, поставщики, службы экстренного реагирования, подрядчики, инспекторы регулирующих органов или других компетентных органов), также следует рассматривать как источник потенциальной угрозы, создаваемой внутренним нарушителем.

КАТЕГОРИИ ВНУТРЕННИХ НАРУШИТЕЛЕЙ

2.9. Невольный внутренний нарушитель — это внутренний нарушитель без намерения и мотивации для совершения злоумышленного действия, который используется злоумышленником без ведома этого невольного внутреннего нарушителя. Например, при компьютерной атаке невольный внутренний нарушитель может не знать, что определенные действия (например, нажатие на вредоносную ссылку в электронном письме, замаскированном под надежный источник) могут позволить злоумышленнику получить информацию или доступ с проверкой подлинности.

2.10. Внутренний нарушитель — это нарушитель, который совершает злоумышленные действия осознанно, с умыслом и мотивацией. Внутренний нарушитель может быть пассивным или активным, а активный внутренний нарушитель может действовать насильственными, либо ненасильственными методами. Такую категоризацию целесообразно применять при проведении оценки, например, при составлении профилей нарушителей в оценке угроз или проектной угрозе (ПУ), либо при разработке сценариев, которые будут использоваться для проверки мер физической ядерной безопасности как части процесса оценки систем физической ядерной безопасности.

2.11. Пассивный внутренний нарушитель оказывает помощь другому нарушителю путем передачи ему информации, которая будет использоваться для совершения злоумышленного действия. Пассивный внутренний нарушитель не участвует в злоумышленном действии каким-либо иным образом и, скорее всего, откажется от своего участия, если возникнет высокая вероятность его идентификации.

2.12. Активный ненасильственный внутренний нарушитель использует скрытность или обман для облегчения или совершения злоумышленного действия и может передавать информацию другому нарушителю. Например, активный ненасильственный внутренний нарушитель может пытаться совершить внезапное хищение или хищение на протяжении длительного времени ядерного материала, или же может оказывать помощь внешним нарушителям в совершении злоумышленного действия путем отключения или игнорирования сигналов тревоги или открытия дверей. Вероятнее всего, активный ненасильственный внутренний нарушитель прекратит совершение злоумышленного действия в случае возникновения высокой вероятности его идентификации (т.е. этот тип внутреннего нарушителя допускает риск выявления действия, но, скорее всего, не пойдет на риск быть идентифицированным).

2.13. Активный насильственный внутренний нарушитель похож на активного ненасильственного внутреннего нарушителя, но готов использовать физическую силу против персонала для содействия в совершении или совершения злоумышленного действия. В зависимости от обстоятельств внутренний нарушитель может переходить от ненасильственных действий к насильственным.

ИДЕНТИФИКАЦИЯ ПОТЕНЦИАЛЬНЫХ УГРОЗ, СОЗДАВАЕМЫХ ВНУТРЕННИМ НАРУШИТЕЛЕМ

2.14. Руководящий материал, изложенный в данном разделе, предназначен в помощь оператору в идентификации потенциальных угроз, создаваемых внутренним нарушителем, и его следует использовать в сочетании с другими методами идентификации угроз со стороны внутренних нарушителей, такими как разработка и анализ вероятных сценариев в рамках оценки системы обеспечения физической ядерной безопасности.

2.15. В [2] рекомендуется: «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*[3]». Государству следует рассматривать атрибутивные признаки, мотивацию и категории внутренних нарушителей и отражать любые вероятные угрозы со стороны внутренних нарушителей в национальной оценке угроз или ПУ.

2.16. Оценка угроз и рисков позволяет также идентифицировать потенциальные угрозы, создаваемые внутренним нарушителем. В дополнение к общей информации об угрозах со стороны внутренних нарушителей, содержащейся в национальной оценке угроз или ПУ, при проведении оценки для конкретной установки следует учитывать информацию о локальных угрозах в месте расположения установки. Эта информация помогает выявить требующие внимания условия (например, уровень преступности) или ситуации, сложившиеся за пределами установки (например, общее отношение общества, наличие организованных враждебно настроенных групп), которые могут способствовать действиям внутренних нарушителей.

2.17. Потенциальные угрозы со стороны внутренних нарушителей также могут быть идентифицированы путем определения внутренних нарушителей, имеющих удаленный или внутренний санкционированный доступ к системам установки через компьютерные сети. Современные системы установки, в том числе системы, которые используются для обеспечения физической ядерной безопасности, базируются на компьютерных средствах управления и сетях. Защиту этих систем от компьютерных атак следует обеспечивать, как указано в [7]. При идентификации угроз, создаваемых внутренним нарушителем, следует изучать персонал, имеющий доступ к таким системам.

3. ИДЕНТИФИКАЦИЯ ЦЕЛЕЙ

3.1. При идентификации целей для совершения злонамеренных действий, как изложено в [15], определяются материал и оборудование, для которых

---

[3] В ПУ указываются «Признаки и характеристики потенциальных *внутренних нарушителей* и/или внешних нарушителей, могущих совершить попытку *несанкционированного изъятия* или *саботажа* (диверсии), для противодействия которым создается и оценивается *система физической защиты*».

необходимо обеспечивать защиту от действий со стороны нарушителя. Цели могут включать ядерный материал, связанные с ним места его размещения, здания, оборудование, отдельные компоненты, информацию, системы и функции. Руководящие материалы по идентификации целей применительно к установкам и ядерному и радиоактивному материалу содержатся в [2–4, 8, 15, 16].

3.2. Защита может также требоваться для устройств или активов (например, систем наблюдения, портальных мониторов), которые сами по себе не определяются как цели, но имеют важное значение для защиты идентифицированных целей. Внутренний нарушитель может попытаться действовать в обход или скомпрометировать такие устройства или активы при совершении злоумышленного действия.

ЦЕЛИ ДЛЯ СОВЕРШЕНИЯ НЕСАНКЦИОНИРОВАННОГО ИЗЪЯТИЯ

3.3. Ядерный материал как цель несанкционированного изъятия может быть отнесен к одной из трех категорий (I–III) в зависимости от относительной привлекательности и характеристик ядерного материала, а также от потенциальных последствий в случае его использования в ядерном взрывном устройстве. Эта категоризация представлена в таблице 1 [2]. Следует также рассматривать возможность несанкционированного изъятия ядерного или радиоактивного материала для создания радиологического диспергирующего устройства [3]. Помимо ядерного и другого радиоактивного материала целями хищения могут быть чувствительная информация и активы чувствительной информации.

3.4. При идентификации потенциальных целей для совершения внутренним нарушителем несанкционированного изъятия ядерного материала следует учитывать возможность как внезапного хищения, так и хищения, совершаемого на протяжении длительного времени. «Внезапное хищение» — это несанкционированное изъятие целевого или значительного количества ядерного материала в течение одного эпизода. «Хищение на протяжении длительного времени» представляет собой многократное несанкционированное изъятие предположительно небольших количеств ядерного материала из одного или нескольких мест.

3.5. Внутренний нарушитель может осуществлять хищение ядерного материала на протяжении длительного времени, с тем чтобы оставаться

незамеченным, совершая при этом многократные изъятия малых количеств материала ниже порога обнаружения СУиК ЯМ и систем физической защиты. Хищение на протяжении длительного времени может осуществляться либо путем удаления ядерного материала из установки при каждой операции приобретения, либо путем накопления ядерного материала в скрытом месте для его последующего, возможно, внезапного удаления из установки. При идентификации цели следует учитывать возможность того, что внутренний нарушитель сможет собрать количество ядерного материала, соответствующее более высокой категории, путем накопления достаточного количества ядерного материала более низкой категории. В процессе идентификации цели и определения возможности и вероятности реализации сценария хищения на протяжении длительного времени следует также рассматривать такие параметры, как элементный состав, физическая форма материала, способы его использования, используемое в технологическом процессе количество и находящееся на хранении количество. Аналогичные параметры следует рассматривать и применительно к случаям внезапного хищения.

ЦЕЛИ ДЛЯ СОВЕРШЕНИЯ САБОТАЖА

3.6. Цели для возможного совершения саботажа на установке идентифицируются в результате анализа потенциальной возможности того, что определенное инвентарное количество радиоактивного материала и радиоактивных отходов на установке, включая ядерный материал и радиоактивные источники [3], может привести к возникновению неприемлемых радиологических последствий или серьезных радиологических последствий. Более подробная информация о мерах по физической ядерной безопасности, которые следует принимать для защиты от саботажа, а также для проведения анализа целей для совершения саботажа, изложена в [2, 15].

3.7. Следует обеспечивать, чтобы процесс идентификации целей включал определение возможных комбинаций действий (сценариев), которые может предпринять внутренний нарушитель для деградационного воздействия на конструкции, системы и элементы установки, которое может привести к неприемлемым радиологическим последствиям или серьезным радиологическим последствиям.

ИДЕНТИФИКАЦИЯ СИСТЕМ, ИСПОЛЬЗУЕМЫХ ДЛЯ ОБЕСПЕЧЕНИЯ ФИЗИЧЕСКОЙ ЯДЕРНОЙ БЕЗОПАСНОСТИ

3.8. Следует обеспечивать, чтобы процесс идентификации целей охватывал все системы, которым может потребоваться дополнительная защита от угроз со стороны внутреннего нарушителя. Системы физической защиты, СУиК ЯМ, а также системы безопасности и управления процессами следует рассматривать в качестве потенциальных целей для совершения злоумышленных действий, в том числе инициированных внутренним нарушителем.

3.9. Внутренний нарушитель может иметь санкционированный доступ к установке или к информации об установке и может совершать атакующие действия в отношении других конструкций, систем или элементов с целью косвенного совершения конечной атаки, маскировки злоумышленных действий или оказания содействия внешнему нарушителю. В зависимости от установки или операций на установке внутренний нарушитель может использовать компьютерные системы (например, для получения чувствительной информации могут использоваться внутриучрежденческие сети или коммуникационные компьютеры).

3.10. Компрометация компьютерных систем на установке может негативно повлиять на безопасность, физическую безопасность ядерного материала или меры по смягчению последствий аварии. Оператору следует проводить соответствующую оценку и обеспечивать защиту компьютерных систем, которые содержат информацию, относящуюся к безопасности или физической безопасности, соразмерно с риском и потенциальными последствиями утечки такой информации. Следует обеспечивать, чтобы эта оценка была нацелена на выявление критических компьютерных систем, которые могут быть наиболее уязвимыми для злоумышленных действий и отказ которых может привести к событию, связанному с физической ядерной безопасностью.

3.11. Оператору следует рассматривать целесообразность проведения дополнительного обучения сотрудников и подрядчиков, имеющих доступ к чувствительным системам, для повышения их информированности по вопросам физической безопасности. Внешние нарушители могут пытаться использовать внутренних нарушителей, имеющих доступ к установке, чувствительной информации, активам чувствительной информации или сетям установки, для получения помощи или содействия в совершении злоумышленных действий или в их маскировке.

4. МЕРЫ, НАПРАВЛЕННЫЕ НА ПРОТИВОДЕЙСТВИЕ ПОТЕНЦИАЛЬНЫМ УГРОЗАМ, СОЗДАВАЕМЫМ ВНУТРЕННИМ НАРУШИТЕЛЕМ

4.1. В число мер по обеспечению физической ядерной безопасности, используемых для защиты от угроз со стороны внутреннего нарушителя, следует включать как предупредительные, так и защитные меры. Термин «предупредительные меры» относится к мерам, применение которых направлено на сокращение числа потенциальных внутренних нарушителей на этапе до предоставления сотрудникам доступа, на минимизацию возможностей для внутреннего нарушителя совершить злоумышленное действие при наличии доступа или на предотвращение совершения потенциальным внутренним нарушителем злоумышленного действия. Термин «защитные меры» используется для описания мер, направленных на выявление или задержку осуществления злоумышленных действий, реагирование на злоумышленные действия или на смягчение последствий злоумышленного действия.

4.2. Настоящее руководство не охватывает весь спектр мер, которые могут применяться для противодействия угрозам, создаваемым внутренним нарушителем. Тем не менее, если угроза правильно определена, процесс идентификации целей является достаточно полным и меры эффективно осуществляются и оцениваются, применение предупредительных и защитных мер позволяет обеспечить противодействие угрозам, создаваемым внутренним нарушителем.

4.3. Компетентным органам следует собирать информацию о мерах, применяемых для противодействия угрозам, создаваемым внутренним нарушителем, и об инцидентах, связанных со злоумышленными действиями внутренних нарушителей, с целью анализа тенденций, слабых мест и надлежащей практики. В соответствующих случаях эту информацию следует передавать компетентным международным учреждениям для выработки более полного понимания масштаба и характера проблем в обеспечении физической безопасности, создаваемых внутренними нарушителями.

ОБЩИЙ ПОДХОД К РЕАЛИЗАЦИИ

4.4. Как указано в [2], требования к физической ядерной безопасности следует основывать на дифференцированном подходе, учитывая результаты последней оценки угроз, относительную привлекательность и характеристики материала и возможные последствия, связанные с несанкционированным изъятием ядерного материала или с саботажем в отношении ядерного материала или ядерных установок. Общие руководящие материалы по реализации дифференцированного подхода к защите ядерных материалов и установок от угроз со стороны внутреннего нарушителя и внешних угроз изложены в [15].

4.5. Реализация мер по обеспечению физической ядерной безопасности с целью защиты от угроз со стороны внутреннего нарушителя включает выбор комбинации предупредительных и защитных мер[4] и их применение в соответствии с дифференцированным подходом. Для достижения требуемого эффекта важно, чтобы выбранные меры осуществлялись и оценивались эффективно. Не все меры подходят для конкретной установки или операции.

4.6. Следует обеспечивать, чтобы эшелоны (уровни) предупредительных и защитных мер применялись в соответствии с концепцией глубокоэшелонированной защиты так, чтобы внутренние нарушители для достижения своих целей были вынуждены преодолевать или обходить несколько эшелонов мер или технических средств. Эти эшелоны могут состоять из административных мер (например, процедуры, инструкции, правила контроля доступа, правила обеспечения конфиденциальности), технических мер или их сочетания. Оба типа этих мер следует применять так, чтобы обеспечивалась их интеграция с персоналом и оборудованием.

4.7. Оператору следует разрабатывать план обеспечения физической безопасности при подаче заявки на получение лицензии, как указано в [2], в котором следует указывать меры, необходимые для противодействия угрозам, создаваемым внутренним нарушителем, включая меры, направленные на противодействие угрозам, создаваемым внутренним нарушителем в отношении информационной и компьютерной безопасности (например, кибератакам, которые могут совершать внутренние нарушители [7, 8]). Оператору следует проводить рассмотрение угроз со стороны внутреннего

---

[4] Некоторые меры могут оказывать как предупредительное, так и защитное действие.

нарушителя на этапах проектирования, оценки, реализации и обслуживания систем физической ядерной безопасности на уровне установки.

4.8. План обеспечения физической безопасности следует составлять так, чтобы он указывал, как системы физической ядерной безопасности будут реализованы на установке, а также предусматривал меры, предназначенные для защиты идентифицированных целей от угроз со стороны внутреннего нарушителя. В план следует включать информацию об этих мерах. Например, технические меры могут включать меры по сохранению и наблюдению, предназначенные для выявления и задержки действий внутреннего нарушителя, меры по мониторингу и усилению защиты сетей и связанных с ними устройств, а также меры по обеспечению контроля доступа. Административные меры могут включать процедуры, инструкции, административные санкции, правило двух лиц, правила конфиденциальности и административные проверки, а также плановые, внеплановые или необъявленные инспекционные проверки осуществления предупредительных и защитных мер. Инспекционные проверки следует проводить силами оператора или с привлечением независимых групп. В плане обеспечения физической безопасности следует указывать, как будет проводиться оценка таких мер (см. раздел 5).

4.9. В рамках реагирования на возникающие новые угрозы со стороны внутреннего нарушителя на существующих и находящихся в эксплуатации установках может требоваться модернизация систем обеспечения физической безопасности.

РЕАЛИЗАЦИЯ МЕР, НАПРАВЛЕННЫХ НА ПРОТИВОДЕЙСТВИЕ УГРОЗАМ, СОЗДАВАЕМЫМ ВНУТРЕННИМ НАРУШИТЕЛЕМ

4.10. Для защиты от потенциальных угроз, создаваемых внутренним нарушителем, следует применять как предупредительные, так и защитные меры. Предупредительные меры могут применяться для:

a) уменьшения потенциальных угроз со стороны внутреннего нарушителя до предоставления сотрудникам соответствующего доступа путем выявления нежелательного поведения или характеристик, которые могут указывать на мотивацию;
b) дальнейшего уменьшения потенциальных угроз со стороны внутреннего нарушителя после предоставления сотрудникам

соответствующего доступа путем выявления нежелательного поведения или характеристик, которые могут указывать на мотивацию;

c) сведения к минимуму возможностей для совершения злоумышленных действий путем ограничения доступа, полномочий и знаний, которые могут иметь внутренние нарушители.

Защитные меры могут применяться для:

1) выявления, задержки осуществления злоумышленных действий и реагирования на эти действия;
2) смягчения или минимизации последствий событий, связанных с физической ядерной безопасностью, и при необходимости для определения места нахождения или возвращения материала.

На рис. 1 показано как эти действия в рамках указанных мер могут применяться в целях противодействия угрозам, создаваемым внутренним нарушителем.

4.11. Многие меры, указанные в следующих ниже двух подразделах, могут рассматриваться как предупредительные, так и защитные. При выборе и оценке мер следует учитывать потенциальную ценность каждой предлагаемой меры с точки зрения как защиты, так и предупреждения.

Применение предупредительных мер

4.12. Целью предупредительных мер является уменьшение числа потенциальных угроз со стороны внутреннего нарушителя и сведение к минимуму возможностей совершения внутренними нарушителями

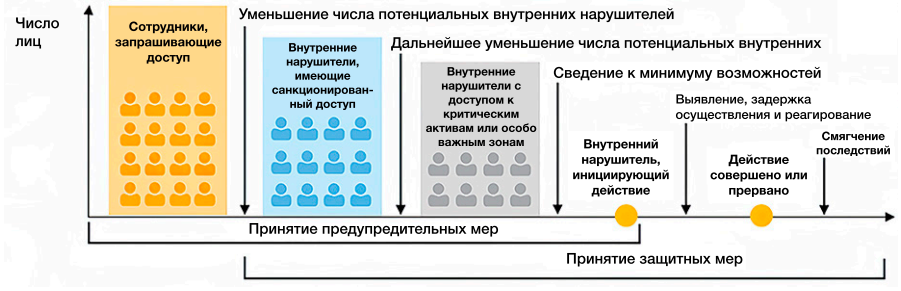

РИС. 1. Действия, применяемые в рамках предупредительных и защитных мер, направленных на противодействие потенциальным угрозам, создаваемым внутренним нарушителем.

злоумышленных действий. Предупредительные меры следует применять на этапах при приеме на работу, в течение трудовой деятельности и при увольнении. Кроме того, предупредительные меры включают меры по обеспечению качества и специальные меры по обеспечению компьютерной безопасности. Следует обеспечивать, чтобы операторы применяли предупредительны меры, изложенные в настоящем разделе.

Меры, применяемые при приеме на работу

4.13. Следует обеспечивать, чтобы лица, принимаемые на работу, требующую доступа на установку, проходили проверку (верификацию) личности, проверку (верификацию) личных документов и оценку благонадежности.

4.14. Проверка личности применяется для подтверждения того, что персональные данные проверяемого лица верны и подлинны.

4.15. Проверка личных документов предназначена для установления подлинности сведений об истории трудовой деятельности кандидата, о его образовании и квалификации, необходимой для выполнения данной работы. Проверка (верификация) и подтверждение (валидация) документов и квалификационных данных может осуществляться путем обращения за справкой к предыдущим работодателям, учебным заведениям и лицам, давшим характеристику-рекомендацию.

4.16. Оценки благонадежности включают проведение первоначальной оценки (при приеме на работу) и оценок на постоянной основе (периодически в течение всего периода трудовой деятельности данного лица) добросовестности, честности и надежности сотрудника. Рекомендация, изложенная в [2], гласит:

> «С учетом государственного законодательства, регулирующих правил или политики в отношении неприкосновенности частной жизни и должностных требований государству следует определять политику обеспечения благонадежности, имеющую целью установление обстоятельств, при которых требуется проверка благонадежности и методов ее обеспечения, с использованием *дифференцированного подхода*».

4.17. В ходе оценки следует проверять законопослушность данного лица и соблюдение этим лицом правил, действующих на установке, а также рассматривать любые требующие внимания поведенческие или

мотивационные факторы. Например, при проведении оценки следует ставить задачу выявления таких мотивационных факторов, как финансовые проблемы или трудности (например, долги, сокращение заработной платы), увлеченность проблемной идеологией, желание мести (например, из-за субъективно ощущаемой несправедливости), физическая зависимость (например, наркотики, алкоголь, секс), психологическое или психическое состояние, серьезная неудовлетворенность личной или профессиональной жизнью, а также другие факторы, из-за которых данное лицо может быть склонено или принуждено к совершению злоумышленного действия. Эти мотивационные факторы могут быть выявлены в результате проверки такой информации, как сведения об уголовном преследовании, характеристики-рекомендации, выданные индивидуальными лицами и организациями, сведения о предыдущей трудовой деятельности, данные финансовых органов, данные о пользовании онлайновыми и другими социальными сетями, сведения из медицинских документов или результаты профессиональной аттестации, а также информация от коллег о наблюдаемом поведении.

4.18. Национальные законы могут ограничивать объем или проведение в данном государстве проверки личности, проверки личных документов и оценку благонадежности.

Меры, применяемые в течение трудовой деятельности

4.19. К сотрудникам, прошедшим проверки перед приемом на работу и получившим санкционированный доступ, в том числе к критически важным активам, чувствительной информации и особо важным зонам, следует применять меры, изложенные в следующих ниже пунктах.

4.20. Следует разработать и применять процедуры сопровождения. Для лиц, благонадежность которых не была определена или которым для выполнения профессиональных обязанностей не требуется оценка благонадежности (например, временного ремонтного персонала, административного персонала, персонала, выполняющего работы по техническому обслуживанию, строительных рабочих, посетителей), при их входе в особо важные или внутренние зоны следует предусматривать сопровождение сотрудниками, имеющими санкционированный доступ и могущими входить в эти зоны без сопровождения. Следует обеспечивать, чтобы сопровождающий сотрудник был информирован о разрешенных действиях, в том числе о том, к каким зонам и системам сопровождаемому лицу разрешен доступ и какие действия ему разрешено выполнять.

4.21. Следует периодически проводить повторные проверки благонадежности сотрудников в течение их трудовой деятельности. Некоторые требующие внимания модели поведения и мотивационные факторы могут оставаться незамеченными или могут проявляться с течением времени. Например, выборочное тестирование на употребление наркотиков или алкоголя во время рабочей смены следует рассматривать как метод оценки благонадежности сотрудника. Степень проверок благонадежности следует дифференцировать в соответствии с уровнем доступа и полномочий, которые сотрудник получает в отношении данной установки и ее активов. Например, для штатных сотрудников, которые являются администраторами сетей, обеспечивают предоставление удаленного доступа к чувствительной информации и работают с ядерным материалом, следует предусматривать проведение более частых и более тщательных проверок благонадежности, чем для сотрудников, работающих в кадровых службах.

4.22. У сотрудников, чья оценка благонадежности ухудшилась в силу личных обстоятельств, уровень доступа может быть временно понижен, или они могут быть отстранены от исполнения управленческих обязанностей до проведения повторной оценки. Для поддержания благонадежности сотрудников могут применяться программы повышения информированности по вопросам физической безопасности, а также меры по обеспечению удовлетворенности работой и поощрения сотрудников, как указано ниже.

4.23. Следует обеспечивать конфиденциальность чувствительной информации таким образом, чтобы разрешение на доступ к этой информации получали исключительно лица, которым полагается ее знать в силу служебной необходимости. Получение информации о чувствительных целях или о процедурах или мерах физической безопасности (например, о местонахождении инвентарного количества ядерного материала или о планах и графиках его транспортировки) может способствовать успешному совершению внутренним нарушителем злоумышленного действия. Следует вести учет лиц, получающих доступ к чувствительной информации, включая дату и время доступа к информации, а также обеспечивать защиту таких учетных документов от внесения в них изменений. Следует обеспечивать надежную защиту и разделение информации о потенциальных слабых местах в системах физической ядерной безопасности (как указано в пункте 4.30), поскольку такая информация может облегчать несанкционированное изъятие или совершение акта саботажа.

4.24. Следует контролировать доступ к ядерным установкам, ядерному материалу, системам ядерных установок и чувствительной информации. Следует разработать и применять документированный процесс санкционирования и аннулирования такого доступа. Этот процесс следует применять к любому лицу, которому необходим удаленный, либо очный доступ на установку или к операциям на установке, включая транспортирование. Верификацию личных данных человека можно проводить с применением выданных государственным органом документов, удостоверяющих личность, и биометрических методов (например, путем сканирования сетчатки глаз, по отпечатку ладони, отпечаткам пальцев, с применением системы распознавания лица). Следует обеспечивать, чтобы процесс основывался на строгом применении принципов «служебной необходимости знать» и «служебной необходимости доступа» согласно тому, как это будет определено компетентным органом. Доступ без сопровождения следует разрешать только в те зоны, вход в которые необходим сотруднику для выполнения порученной работы. Число лиц, имеющих санкционированный доступ к особо обозначенным зонам, следует ограничивать до необходимого минимума.

4.25. В целях сведения к минимуму возможности несанкционированного изъятия материала, а также выявления несанкционированных действий перед обработкой или перемещением ядерного и другого радиоактивного материала следует получать разрешение на осуществление операций по обработке или перемещению [6, 13]. Например, оператору установки следует иметь оформленную в письменной форме процедуру, определяющую, кто может извлекать ядерный материал из хранилища для выполнения операций по обработке, когда его можно извлекать и как это извлечение следует санкционировать и регистрировать. Составляемый на ежедневной или еженедельной основе график работ, координируемых и утверждаемых сотрудниками, отвечающими за выполнение операций, позволяет сократить возможности для несанкционированных действий со стороны персонала, который обычно выполняет эти работы.

4.26. Следует обеспечивать разделение физических зон, обязанностей, времени работы и информации таким образом, чтобы отдельно взятому сотруднику не предоставлялись доступ, полномочия или знания, достаточные для совершения злоумышленного действия. Такое разделение увеличивает объем усилий, которые внутреннему нарушителю необходимо будет приложить для совершения злоумышленного действия, и повышает вероятность того, что внутренний нарушитель должен будет выйти за

рамки своих обычных санкционированных операций в целях совершения злоумышленного действия.

4.27. Оператору установки следует обеспечивать, чтобы физические зоны были разделены так, чтобы отдельно взятый сотрудник не имел доступа ко всем системам, элементам и оборудованию, которые могли бы позволить ему совершить злоумышленное действие. Следует ограничивать число лиц, имеющих доступ к зоне, для которой требуется обеспечивать защиту. Следует установить правила, определяющие круг сотрудников, которым в силу служебной необходимости предоставляется доступ к разделенным зонам; эти правила следует применять ко всем разделенным зонам. Указанные правила следует пересматривать, внося в них соответствующие исправления в случае внесения изменений в процессы или конфигурацию в данной разделенной зоне. Кроме того, следует строго ограничивать число лиц, которым разрешен доступ к каждой из разделенных зон. Для обеспечения соблюдения процедурных требований в отношении применения правил, касающихся доступа, следует проводить инспекции и тестирование эффективности функционирования.

4.28. Разделение обязанностей позволяет разграничивать операции, выполняемые сотрудниками, ограничивая возможности получения внутренним нарушителем санкционированного доступа, полномочий или знаний, достаточных для совершения злоумышленного действия. Разделение обязанностей включает применение принципа наименьших (минимальных) привилегий при работе с компьютерными системами, согласно которому сотрудник получает только привилегии, необходимые ему для выполнения своей работы.

4.29. Время работы следует разделять, ограничивая санкционированный доступ сотрудников в разные рабочие периоды на установке (например, применяя ограничения, связанные с часами работы, выполнением работ по техническому обслуживанию, остановками, нештатными условиями). Например, доступ сотрудника к особо важной зоне следует ограничивать продолжительностью его смены.

4.30. Информацию, хранящуюся как в бумажном, так и в электронном виде, следует делить на раздельно контролируемые части с использованием административных и технических мер для контроля доступа к этой информации. Цель разделения информации на части состоит в том, чтобы не допустить получения внутренними нарушителями полной информации, необходимой для попытки совершения злоумышленного действия.

При разделении информации следует руководствоваться принципом «служебной необходимости знать», который применяется к сотрудникам в отношении чувствительной информации.

4.31. Следует придерживаться стандартных рабочих процедур. Стандартные рабочие процедуры — это письменные инструкции, которые регулируют выполнение неоднократно совершаемых операций в соответствии с утвержденными спецификациями с целью получения определенного результата. Стандартные рабочие процедуры позволяют сводить к минимуму вариации и способствуют обеспечению качества благодаря последовательному осуществлению процессов в организации независимо от кадровых изменений. Применение стандартных рабочих процедур помогает выявлять и, таким образом, предотвращать злоумышленные действия со стороны внутреннего нарушителя, так как эти процедуры обеспечивают базовые рамки для заранее спланированных операций и отклонения от установленной процедуры выполнения операции легче поддаются обнаружению и пресечению другими сотрудниками.

4.32. Следует разрабатывать и вводить в действие программу информированности по вопросам физической безопасности, предназначенную для персонала и подрядчиков. Такая программа обеспечивает повышение культуры физической ядерной безопасности в организации и содействует предупреждению угроз со стороны внутреннего нарушителя, если информированность о таких угрозах для физической безопасности интегрирована в культуру физической ядерной безопасности на установке. Следует обеспечивать, чтобы все сотрудники, независимо от вида выполняемой ими работы или их функций, были информированы об угрозах и потенциальных последствиях злоумышленных действий и о роли, которую сотрудники играют в снижении риска злоумышленных действий. Программы информированности по вопросам физической безопасности могут снизить риск шантажа, принуждения, вымогательства или других угроз в отношении сотрудников и их семей, и следует обеспечивать, чтобы эти программы содействовали тому, чтобы руководству службы безопасности в надлежащих случаях сообщалось о возможных актах запугивания. Программы информированности по вопросам физической безопасности следует разрабатывать в координации с программами информированности по вопросам безопасности в целях поддержания двух эффективных и дополняющих друг друга культур — безопасности и физической безопасности.

4.33. Следует обеспечивать, чтобы программа информированности по вопросам физической безопасности включала четкое изложение политики в области физической безопасности, охватывала меры по обеспечению применения практических методов соблюдения требований физической безопасности, а также непрерывное обучение. Цель обучения сводится к созданию обстановки, в которой все сотрудники информированы о политике и процедурах в области обеспечения физической безопасности, с тем чтобы они могли оказывать содействие в выявлении случаев подозрительного или ненадлежащего поведения и несанкционированных действий и сообщать об этом. В программу обучения следует включать методы оценки информированности по вопросам физической безопасности, а также эффективности обучения и мероприятия по постоянному усовершенствованию или переподготовке. Помимо подготовки персонала к возможности физического инцидента на установке или действий, направленных против активов установки, в обучение следует включать подготовку персонала к возможным кибератакам.

4.34. Следует разрабатывать и вводить в действие программу определения годности к выполнению служебных обязанностей. Следует обеспечивать, чтобы руководители имели подготовку, позволяющую им выявлять требующее внимания поведение сотрудников и обсуждать этот вопрос с соответствующим сотрудником. Программа определения годности к выполнению служебных обязанностей может быть использована также для периодического наблюдения за здоровьем сотрудников. Оператор установки может также рассматривать возможность оказания помощи сотрудникам, находящимся в сложной ситуации (например, в связи с финансовыми, медицинскими, психологическими проблемами).

4.35. Следует обеспечивать, чтобы об инцидентах, связанных с физической безопасностью (т.е. инцидентах на установке, которые связаны с нарушением или несоблюдением правил, относящихся к политике, процедурам или системам обеспечения физической безопасности на установке), составлялись рапорты и проводились расследования этих инцидентов. Составление рапортов об инцидентах и проведение расследования инцидентов, связанных с физической безопасностью, позволяет установкам разрабатывать корректирующие действия и предупреждать угрозы со стороны внутреннего нарушителя. Инцидент может инициироваться внутренним нарушителем и быть предвестником злоумышленного действия в связи с подготовкой к этому действию или попыткой проверить реакцию системы. Тщательное расследование таких инцидентов может служить

сдерживающим фактором для внутренних нарушителей и позволяет выявить сотрудников, которые могут оказаться внутренними нарушителями.

4.36. Сотрудникам следует обеспечивать хорошие условия труда, поощрение за труд и признание достижения хороших результатов в работе. Хорошие условия труда, поощрение и признание результатов являются важной частью поддержания и повышения морального духа и лояльности сотрудников, что способствует формированию эффективной культуры физической безопасности.

4.37. Следует обеспечивать, чтобы сотрудники четко понимали, что в случае преднамеренного нарушения рабочих инструкций, правил или законов будут применяться санкции. Возможное применение дисциплинарных мер или возбуждение судебного преследования может удерживать внутренних нарушителей от совершения злоумышленных действий. Кроме того, требование о том, чтобы операторы сообщали компетентному органу о попытке совершения или о совершении злоумышленных действий может обеспечить после проведения соответствующей аналитической оценки создание базы данных для информационного обмена между операторами, а также может служить источником информации, используемой для целей внесения необходимых изменений в регулирующие требования.

Меры, применяемые при увольнении

4.38. Следует обеспечивать, чтобы права доступа и полномочия сотрудника, включая доступ к компьютеру, аннулировались после увольнения с должности данного лица, прекращения трудовых отношений или расторжения контракта с ним. Следует устанавливать процедуры увольнения, предусматривающие лишение физического доступа к установке; заключение соглашения о неразглашении в целях защиты чувствительной информации; смену ключей шифрования, паролей и кодов доступа.

Политика и программы обеспечения качества

4.39. Следует обеспечивать, чтобы политика и программы обеспечения качества на установке применительно к физической ядерной безопасности были направлены на противодействие угрозам, создаваемым внутренним

нарушителем, согласно оценке угроз или проектным угрозам (ПУ). Пункт 3.52 в [2] гласит:

> «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».

4.40. Программы обеспечения качества следует разрабатывать так, чтобы они охватывали все системы установки, используемые для обеспечения физической ядерной безопасности, с целью адекватной защиты от угроз со стороны внутреннего нарушителя. В программах обеспечения качества следует предусматривать управление конфигурацией систем физической ядерной безопасности, обеспечивающее непрерывное функционирование этих систем в соответствии с требуемыми критериями эффективности функционирования и позволяющее понимать любые потенциальные последствия внесения в системы изменений, например, внутренним нарушителем.

Меры, применяемые для защиты компьютерных систем

4.41. Определенные меры, такие как сопровождение, могут быть эффективными средствами ограничения доступа внутреннего нарушителя к ядерному и радиоактивному материалу, однако они не обеспечивают достаточную защиту от потенциальных внутренних угроз для компьютеров и систем, построенных на базе компьютерных сетей; такая защита может быть обеспечена мерами информационной безопасности [7, 8]. Например, третьи стороны и поставщики могут иметь на установке физический доступ к чувствительной информации и оборудованию при проведении работ по созданию и обслуживанию компьютерных и сетевых систем. Эти третьи стороны и поставщики могут запрашивать удаленный доступ на всех этапах жизненного цикла сетевых систем, и решение по предоставлению им такого доступа следует принимать только на основе использования риск-информированного подхода [1].

4.42. Оператору установки следует разрабатывать и применять политику, определяющую допустимое использование компьютерных систем.

В этой политике могут быть зафиксированы одобренные процедуры использования компьютеризированных систем, изложены требования работодателя в отношении мониторинга одобренного использования этих систем, предусмотрены мероприятия по обучению, а также четко указаны действия, которые запрещается выполнять на компьютерных системах. Оператору установки следует также рассмотреть возможность использования технических мер для обеспечения соблюдения или улучшения политики в области работы с системами. Например, оператор установки может разработать политику в отношении социальных сетей, а также провести компьютерное обучение по пользованию социальными сетями, направленное на снижение вероятности использования внутренних сотрудников лицами со злоумышленными намерениями в качестве невольных внутренних нарушителей.

Применение защитных мер

4.43. Цель защитных мер, направленных на противодействие угрозам, создаваемым внутренним нарушителем, это — выявление, задержка осуществления злоумышленных действий и реагирование на эти действия после начала их осуществления; реагирование может включать смягчение последствий и возвращение под контроль ядерного или радиоактивного материала. При разработке и реализации защитных мер следует обеспечивать, чтобы эти меры поддерживали функционирование и содействовали обеспечению безопасности установки и не оказывали негативного воздействия на ее функционирование и безопасность. В случае коллизии требований, особенно в том, что касается безопасности, следует принимать решение, которое сводит к минимуму совокупный риск для персонала и населения и обеспечивает достаточный уровень физической безопасности.

4.44. Защитные меры, направленные на противодействие угрозам, создаваемым внутренним нарушителем, следует применять с использованием дифференцированного подхода в отношении идентифицированных целей. В дополнение к защите от несанкционированного изъятия ядерного материала, как указано в пункте 5.12 в [2]: «*Оператору* следует разрабатывать *систему физической защиты*, которая будет эффективно противодействовать реализации выявленных сценариев *саботажа* (диверсии) и соответствовать требуемому уровню защиты для *ядерной установки* и *ядерного материала*». В число сценариев саботажа следует включать сценарии с участием одного или нескольких внутренних нарушителей. В

следующих ниже подразделах указаны меры защиты от угроз со стороны внутренних нарушителей, применение которых следует рассматривать при проектировании системы физической ядерной безопасности.

Меры выявления

4.45. Выявление попыток злоумышленных действий со стороны внешних нарушителей направлено на обнаружение вторжения в любую из защитных мер установки. Вместе с тем внутренние нарушители могут действовать в обход или отключить определенные меры физической защиты и СУиК ЯМ в силу наличия у них санкционированного доступа, полномочий и знаний. Операторам следует применять множественные и разнообразные защитные меры для этих систем с целью выявления потенциальных злоумышленных действий, совершаемых внутренним нарушителем, а также следует предоставлять необходимую для расследования и анализа информацию. Оператору установки следует проводить всестороннее изучение всей информации, получаемой в результате реализации этих мер выявления. Отдельные сигналы, которые представляются незначительными, могут служить индикацией признаков злоумышленного действия при их рассмотрении в совокупности.

4.46. Расследование может включать просмотр видеозаписей и изучение данных сетевого мониторинга, проверку устройств индикации вмешательства или данных измерений, связанных с ядерными материалами, проверку журналов регистрации доступа или проведение экстренной проверки инвентарного количества. Следует обеспечивать, чтобы персонал, проводящий расследование и анализ возможного злоумышленного действия, имел соответствующую квалификацию. От сроков проведения расследования и анализа после выявления напрямую зависят возможности оператора установки своевременно реагировать на злоумышленное действие.

4.47. Следует выявлять и расследовать подозрительные или несанкционированные действия, так как они могут свидетельствовать о том, что злоумышленный акт находится на разведывательной или подготовительной стадии. Например, внутренний нарушитель может попытаться действовать в обход установленных процедур (например, пронести запрещенные предметы в зону), проникнуть в зону, доступ к которой ему не разрешен (например, войти через аварийную дверь), вызвать срабатывание тревожной сигнализации

для хронометража и определения характера мер реагирования или получить чувствительную или другую информацию, доступ к которой регулируется на основе принципа «служебной необходимости знать» и отсутствует у внутреннего нарушителя.

4.48. Защитные меры, предназначенные для выявления угроз со стороны внутренних нарушителей, необходимо разрабатывать так, чтобы они обеспечивали выявление, правильную оценку и составление рапортов о подозрительных или злоумышленных действиях. Применяемые на установке меры выявления угроз со стороны внутреннего нарушителя, как правило, включают меры, предусматривающие контроль доступа, отслеживание местонахождения персонала, обнаружение запрещенных предметов, наблюдение, применение СУиК ЯМ и средства обеспечения компьютерной безопасности. Описание этих мер приводится ниже.

Контроль доступа

4.49. Оператору следует установить и задокументировать строгие правила и процедуры контроля доступа к ядерному материалу, оборудованию, используемому для обработки ядерных материалов или выполнения технологических операций с ним (физического манипулирования), и к данным о ядерном материале или системах, имеющих отношение к безопасности или физической безопасности. Строгое выполнение правил и процедур контроля доступа позволяет сводить к минимуму доступ внутренних нарушителей к материалу, системам и оборудованию. Правила и процедуры контроля доступа могут также служить в качестве сдерживающего фактора, обусловленного возможностью обнаружения или идентификации внутреннего нарушителя при совершении им попытки получить доступ к материалам, оборудованию или данным, который ему не разрешен.

4.50. Следует обеспечивать, чтобы правила и процедуры контроля доступа применялись в различных ситуациях, включая выдачу разрешения на доступ к зонам, содержащим ядерный материал, и контроль ядерного материала в штатных и нештатных условиях, таких как реальные или симулируемые (учебные) аварийные ситуации. Например, правила контроля доступа могут применяться к контролю и раздаче комбинаций ключей и замков в системах ручного контроля доступа, а также к печати карточек-пропусков, регистрации личных идентификационных номеров при приеме на работу, сбору биометрических данных и контролю замков в электронных системах.

4.51. Оператору следует обеспечивать защиту от несанкционированного доступа к: a) оборудованию, предназначенному для печати карточек-пропусков; b) вспомогательному оборудованию и запасным частям к нему; c) системам, используемым для выдачи официальных разрешений на доступ. Оператору установки следует строго контролировать доступ к оборудованию, используемому для обеспечения физической безопасности, или оборудованию, связанному с обеспечением физической безопасности, проведением работ по калибровке и техническому обслуживанию. Оператору также следует разрабатывать и вводить в действие процедуры, обеспечивающие целостность этого оборудования. Например, по окончании работ по техническому обслуживанию и до передачи этого оборудования в эксплуатацию следует проводить его тестирование силами персонала, имеющего на это официальное разрешение, с целью проверки отсутствия вмешательства в оборудование.

4.52. Правила контроля доступа следует устанавливать для посетителей и сопровождающих, а также на случай отклонений от нормальных (нештатных) условий, таких как реагирование на аварийные ситуации и сбои в работе систем.

4.53. Перед выдачей официального разрешения на доступ в зону с контролируемым доступом следует проверять соблюдение конкретных критериев, применяемых в отношении персонала, таких как принцип «служебной необходимости знать» и оценка благонадежности. Введение правил контроля доступа следует согласовывать с подразделениями по СУиК ЯМ, эксплуатации, обеспечению безопасности и физической защиты.

4.54. Следует обеспечивать, чтобы каждый доступ или попытка доступа к чувствительным физическим местам и компьютерным системам регистрировались в виде записей в системе контроля доступа. Мониторинг или проверка этих записей в системе контроля доступа позволяет выявлять злоумышленные действия, совершаемые внутренними нарушителями. Например, в результате проверок регистрационных записей в системе контроля доступа могут быть выявлены такие события, как незапланированный доступ к хранилищу, неудачные попытки ввода персонального идентификационного номера, отрицательный результат биометрической аутентификации при использовании карточки-пропуска с санкционированным доступом или другие признаки попыток проникновения лиц, не имеющих санкционированного доступа. Нарушения или подозрительная активность после их выявления могут быть оценены как потенциальные злоумышленные действия. При проектировании или

модернизации систем меры выявления и связанные с ними процедуры, используемые для мониторинга и проверки записей в системе контроля доступа, следует рассматривать как технические и административные меры контроля доступа.

4.55. В системе контроля доступа следует вести регистрационные записи также в отношении всех лиц, получивших доступ к особо важным зонам или имеющих доступ к ключам, карточкам-ключам или другим средствам подтверждения полномочий (учетным данным), или получивших их в пользование, которые необходимы для доступа к другим системам, включая компьютерные системы, контролирующие доступ к внутренним зонам, особо важным зонам и другим зонам, содержащим ядерный материал [2].

4.56. Соответствующим образом задокументированные записи в системе контроля доступа могут использоваться при проведении расследования в отношении злоумышленного действия для определения круга возможных подозреваемых. В целях выявления потенциальных злоумышленных действий следует также рассматривать и проверять как одобренные, так и отклоненные запросы на санкционированный доступ к режимным зонам или системам, имеющим отношение к обеспечению ядерной или физической безопасности.

Отслеживание местонахождения персонала

4.57. Отслеживание перемещения и местонахождения персонала на установке позволяет оператору обнаруживать попытки нарушения или фактическое нарушение правил контроля доступа, например выход нескольких человек из помещения установки с использованием одной и той же карточки-пропуска. Существующие технологии обеспечивают контроль перемещения людей в режиме реального времени или постфактум, записывая места и зоны, которые они посещают каждый день, а также фиксируя время и продолжительность каждого посещения.

4.58. Информация о том, что на установке имеется система отслеживания местонахождения, может удерживать внутренних нарушителей от совершения несанкционированных действий. Более того, данные системы отслеживания и регистрационные записи системы контроля доступа могут использоваться при проведении расследования злоумышленного действия для целей оценки или после инцидента для составления начального списка подозреваемых лиц.

Обнаружение запрещенных предметов

4.59. Рекомендация, изложенная в пункте 4.43 в [2], гласит:

> «Транспортные средства, лица и упаковки на въезде/входе в *защищенную зону* и *внутреннюю зону* следует подвергать *досмотру* для обнаружения и предупреждения несанкционированного доступа и проноса/доставки запрещенных предметов. Транспортные средства, лица и упаковки на выезде/выходе из *внутренней зоны* следует подвергать *досмотру* для обнаружения и предупреждения *несанкционированного изъятия*».

4.60. Оператору следует составить и задокументировать список предметов, которые запрещается использовать в зонах ограниченного доступа, защищенных зонах, внутренних зонах и особо важных зонах. В число запрещенных предметов могут входить неразрешенные к проносу/провозу устройства и материалы, такие как компьютеры, сотовые телефоны, планшеты и другие носители информации или информационно-технологические устройства, оснащенные камерами; материал защиты от излучения; оружие или взрывчатые вещества. Эти предметы могут использоваться для получения доступа или причинения ущерба чувствительным системам или оборудованию или их компонентам, или для несанкционированного изъятия ядерного материала или саботажа в отношении ядерного материала. В целях обеспечения защиты системы физической защиты, СУиК ЯМ, систем безопасности и эксплуатации или для защиты информации от действий со стороны внутренних нарушителей на установке может быть конкретно определен список других запрещенных предметов.

4.61. Оператору следует немедленно проводить расследование случаев обнаружения запрещенных предметов на входе/въезде в соответствующую зону или выходе/выезде из нее как потенциального злоумышленного действия, совершенного внутренним нарушителем. При подготовке к злоумышленному действию внутренний нарушитель может пытаться проводить тестирование системы выявления запрещенных предметов с целью определения чувствительности детекторов или эффективности процедуры оценки. Следует обеспечивать выявление, оценку, отражение в рапортах и расследование подозрительных или повторяющихся ситуаций обнаружения запрещенных предметов.

4.62. Меры выявления запрещенных предметов включают ручной досмотр персонала, упакованных грузов и транспортных средств (проводимый как на периодической, так и на выборочной основе); применение металлодетекторов, рентгеновских аппаратов и детекторов излучения; использование служебных собак и других средств для обнаружения химических и взрывчатых веществ. При применении этих мер следует учитывать специфические особенности установки и угрозы, от которых требуется обеспечивать защиту в соответствии с оценкой угроз или ПУ, если это применимо.

4.63. Оператору следует разрабатывать и вводить в действие политику, определяющую запрещенные предметы и связанные с ними процедуры поиска и обнаружения. Следует обеспечивать, чтобы персонал, проводящий досмотр или использующий оборудование для выявления запрещенных предметов, был обучен применению данного оборудования и надлежащим образом реагировал в случае обнаружения запрещенного предмета. Реагирование может включать подтверждение исключения, на которое получено официальное разрешение, задержание потенциального внутреннего нарушителя или документирование события с целью последующего выявления потенциальных злоумышленных действий.

4.64. Следует обеспечивать, чтобы строгость досмотров и выбор мест их проведения соответствовали чувствительности зоны, в которой возникла необходимость проведения операции досмотра, и близости этой зоны к цели злоумышленного действия. Досмотры следует проводить в зонах вблизи от места, где возникла необходимость проведения операции досмотра. Для дальнейшего сдерживания несанкционированного изъятия или саботажа в отношении ядерного и радиоактивного материала досмотр следует проводить на периодической и выборочной основе. Досмотры также следует проводить в условиях аварийной эвакуации, включая учения.

4.65. Во время детального досмотра транспортного средства перед погрузкой и отправкой груза следует применять процедуры мониторинга, исключающие возможность для лиц, проводящих досмотр, внести запрещенные предметы, которые могут способствовать совершению злоумышленного действия.

4.66. Для обнаружения несанкционированного изъятия ядерного материала, находящегося у сотрудника, в упаковках или транспортных средствах, на входе/въезде в защищенные, внутренние и особо важные зоны или выходе/выезде из них следует использовать стационарные

или ручные детекторы излучения. С целью повышения эффективности детектирования излучения металлодетекторы следует использовать в сочетании с детекторами излучения на предназначенных для контроля прохода людей входах и выходах, поскольку для блокировки обнаружения радиоактивных сигнатур в случае изъятия ядерного материала из установки может использоваться экранирующий материал.

4.67. Следует разрабатывать и вводить в действие конкретные процедуры подтверждения исключений в отношении проноса/доставки на установку запрещенных или подлежащих контролю предметов (например, радиоактивных калибровочных источников) [3].

Наблюдение

4.68. Меры наблюдения могут применяться для непрерывного мониторинга действий отдельных лиц в особо обозначенных зонах установки, в которых возможно совершение злоумышленных действий, с целью выявления, регистрации и оценки несанкционированных действий.

4.69. В число мер наблюдения входят визуальное наблюдение, видеомониторинг в реальном времени или просмотр видеозаписей, полученных с помощью автоматизированных систем наблюдения. Наблюдение может быть эффективным не только в качестве средства обнаружения, но и средства сдерживания и инструмента расследования потенциальных злоумышленных действий, совершаемых внутренним нарушителем.

4.70. Следует обеспечивать, чтобы персонал, осуществляющий наблюдение, был способен фиксировать санкционированные и выявлять несанкционированные действия, а также имел соответствующие средства для оперативной и безопасной передачи сообщений о любой наблюдаемой несанкционированной деятельности.

4.71. В случае получения сообщения о несанкционированной деятельности видеозаписи с камер наблюдения могут быть использованы для точной оценки злоумышленного действия или выявления возможных подозреваемых лиц. Отсутствие информации наблюдения может осложнять своевременное проведение оценки злоумышленных действий.

4.72. Рекомендация, изложенная в пункте 4.48 в [2], гласит: «когда во *внутренней зоне* присутствует персонал, *обнаружение*

несанкционированного действия следует обеспечивать посредством мер постоянного наблюдения (например, путем соблюдения *правила двух лиц*)». Использование мер наблюдения следует предусматривать при проведении таких операций, как техническое обслуживание, и особенно при выполнении операций по упаковке, отгрузке и перевозке (транспортировке) [14]. Наблюдение может осуществляться с привлечением для этой цели коллег, руководителей, с помощью автоматизированных систем наблюдения или посредством сочетания этих мер.

4.73. Оператору следует устанавливать и проводить периодические проверки, позволяющие подтверждать, что контроль материалов или другие меры защиты применяются в соответствии с установленными процедурами и что оборудование используется правильно.

4.74. Если в зоне (например, содержащей материал категории I) в качестве метода наблюдения применяется правило двух лиц, то физическое местонахождение этих двух лиц, имеющих соответствующее официальное разрешение и обладающих необходимыми знаниями, следует выбирать так, чтобы у этих лиц была беспрепятственная обзорность друг друга и ядерного материала. Кроме того, следует обеспечивать, чтобы эти лица имели соответствующую подготовку и техническую квалификацию, позволяющую им выявлять несанкционированные действия или нарушение процедур. Для эффективности визуального наблюдения следует обеспечивать, чтобы лица, осуществляющие наблюдение, были способны распознавать несанкционированные действия, правильно оценивать ситуацию и своевременно сообщать об этих действиях соответствующим сотрудникам группы реагирования, с тем чтобы эта группа могла предотвратить несанкционированное изъятие. В случае применения при таком наблюдении правила двух лиц необходимо обеспечивать, чтобы оба назначенных для этого специалиста прошли соответствующее обучение, имели беспрепятственную обзорность материала и друг друга при осуществлении наблюдения, а также умели выявлять несанкционированные или осуществляемые с нарушениями процедуры [1].

4.75. Кроме того, правило двух лиц работает эффективно только в случае, когда у этих лиц отсутствует чувство самоуспокоенности, которое может возникать, например, в результате развития дружеских отношений или общения в течение длительного времени. По возможности руководителям следует обеспечивать, чтобы осуществлялась ротация состава таких групп, состоящих из двух человек. Применение правила двух лиц при предоставлении доступа к особо обозначенным зонам может служить

средством сдерживания для внутренних нарушителей и способствовать своевременному выявлению нарушений. В дополнение к этому, правило двух лиц может помочь в обеспечении защиты от вмешательства внутренних нарушителей в системы физической защиты. В случае попыток нарушения правила двух лиц следует составлять рапорт и проводить расследование.

Системы учета и контроля ядерного материала

4.76. Роль, которую СУиК ЯМ играют в обеспечение физической ядерной безопасности, в основном сводится к: получению точных сведений о типе, количестве и местонахождении ядерного материала на установке; эффективному определению фактически наличного количества ядерного материала; обеспечению в определенных случаях применения должного санкционирования действий, выполняемых в отношении ядерного материала [9]. Существует множество мер, использование которых позволяет с помощью СУиК ЯМ выявлять угрозы со стороны внутреннего нарушителя. Эти меры более подробно изложены в [9].

4.77. СУиК ЯМ и другие меры выявления следует также в строгом порядке применять во время выполнения санкционированной операции перевозки (транспортировки) для предотвращения несанкционированного изъятия дополнительного количества ядерного материала с установки внутренним нарушителем или с его помощью. Другие меры выявления могут включать применение: a) правила двух лиц во время подготовки к перемещению материала; b) методов измерения материала; c) устройств индикации вмешательства; d) процедур проверки документов; e) радиационных мониторов; f) стандартных рабочих процедур.

Меры выявления, применяемые для защиты компьютерных систем

4.78. Для выявления злоумышленных действий следует использовать технические меры, охватывающие как аппаратные средства, так и программное обеспечение. Эти меры могут включать, например:

a) установление базового уровня и характеристик для сетевого трафика уязвимых компьютерных активов и проведение проверок базового уровня;
b) применение программных средств выявления вторжений с целью обнаружения моделей поведения пользователей, отклоняющихся от нормальных;

c) мониторинг, контроль и оценку компьютерных систем с целью проверки соблюдения сотрудниками действующей политики и процедур и выявления подозрительных действий. Например, оператор может создавать ложные цели и осуществлять их мониторинг для отслеживания попыток получить несанкционированный доступ к якобы чувствительной информации, тем самым выявляя потенциального внутреннего нарушителя без раскрытия при этом реальной чувствительной информации;

d) введение ограничений в отношении потенциальных путей доступа, которые могут использоваться для получения информации, чтобы только персонал, имеющий на это официальное разрешение, допускался к использованию этих путей, а также обеспечение контроля и мониторинга этих путей в целях защиты от злоумышленного использования. Эти меры могут включать мониторинг, физическую блокировку, запрещение использования съемных носителей информации и мобильных устройств с целью ограничить доступ внутренним нарушителям к чувствительным системам, или создание зон компьютерной безопасности для изоляции систем физической ядерной безопасности и их сетей от других сетей установки [7].

Меры задержки осуществления

4.79. Использование множественных эшелонов различных мер физической защиты или процедурных мер, включая разделение видов работы и обязанностей, может усложнить продвижение внутреннего нарушителя к цели из-за необходимости применения разнообразных средств и специальной подготовки, что обеспечивает дополнительное время и возможности для выявления злоумышленных действий. Благодаря задержке в осуществлении злоумышленного действия, достигаемой таким образом, обеспечивается выявление и обезвреживание внутреннего нарушителя. Создание задержки в осуществлении также может удерживать внутренних нарушителей от попыток совершения злоумышленных действий.

4.80. Меры, применяемые в месте размещения оборудования или ядерного материала (например, крепежные устройства, ограничители, замки), могут быть эффективными средствами задержки осуществления действий внутреннего нарушителя в условиях, когда зона находится под постоянным наблюдением или когда применяются другие надлежащие меры выявления. Такие меры задержки следует разрабатывать так, чтобы внутреннему нарушителю было сложно использовать их с целью отсрочки реагирования на злоумышленное действие, в особенности на акт саботажа.

4.81. Хранение ядерного материала в защищенном месте может увеличить время задержки попытки внутреннего нарушителя совершить злоумышленное действие. В процессе производства или использования минимальное количество ядерного материала, необходимое для производства или использования, следует извлекать из запираемого хранилища за один раз, и следует принимать соответствующие меры контроля ядерного материала между стадиями производственного процесса. Если материал не может быть перемещен в защищенное место хранения на период нерабочего времени, следует принимать дополнительные меры физической защиты и наблюдения до тех пор, пока материал не будет надлежащим образом помещен обратно на хранение в соответствующем защищенном месте.

4.82. Определенные типы мер по задержке осуществления могут вынуждать внутренних нарушителей прибегать к применению более сложных средств, ресурсов, логистики, знаний и навыков для нейтрализации таких мер. Эти сложные ресурсы могут быть недоступны на установке, и, возможно, внутреннему нарушителю потребуется пронести их на установку или получить соответствующий опыт в другом месте.

4.83. Использование конструкций со средствами обеспечения безопасности систем, в которых предусматривается самозащита систем (например, резервирование оборудования, автоматическое отключение оборудования, автоматическое закрытие клапанов), может заставить внутреннего нарушителя прибегнуть к отключению множественных барьеров, состоящих из резервируемых и рассредоточенных систем и оборудования. Такие решения могут обеспечивать задержку в осуществлении злоумышленных действий и препятствовать из успешному совершению. Насколько это возможно, доступ к информации о конструкторских решениях по обеспечению безопасности систем следует ограничивать на основе принципа «служебной необходимости знать», с тем чтобы предотвратить ее использование для совершения злоумышленного действия.

Меры задержки осуществления, предусматриваемые применительно к компьютерным системам

4.84. Меры по обеспечению физической безопасности, применяемые для задержки действий нарушителей, могут не обеспечивать эффективную защиту компьютерных систем вследствие предоставления удаленного доступа к некоторым компьютерным системам и наличия связи между ними. Например, внутренний нарушитель с привилегированным доступом к чувствительным компьютерным системам может в удаленном режиме

одновременно скомпрометировать физически разделенные активы. Меры задержки также могут оказаться неэффективными в случае внутреннего нарушителя, который может использовать действующие полномочия (учетные данные) для получения привилегированного доступа. Таким образом, следует обеспечивать, чтобы меры, применяемые для зашиты компьютерных систем, были направлены на предупреждение и в большей степени на выявление нарушений и реагирование на них.

4.85. Путем соответствующего проектирования и физической реализации проекта зон компьютерной безопасности и эшелонов компьютерной безопасности на установке можно усложнить нарушителю совершение злоумышленного действия с использованием компьютерных систем, а также обеспечить применение средств контроля безопасности, также способных повысить вероятность выявления нарушения [7].

Меры реагирования

4.86. На отклонение от нормы (например, расхождение в инвентарном количестве, открытая дверь, которая должна быть заперта) могут реагировать как эксплуатационный персонал, так и сотрудники службы безопасности. Как правило, эксплуатационный персонал реагирует на отклонение от нормы с целью выяснения причины отклонения. В случае подозрения, что отклонение от нормы связано со злоумышленным действием, следует уведомлять об этом службу безопасности, которая при необходимости осуществляет реагирование. Например:

a) реагирование на действие пассивного внутреннего нарушителя, которое зависит от момента выявления нарушения (времени поступления информации, времени передачи информации или времени завершения расследования);
b) реагирование на действие активного ненасильственного внутреннего нарушителя, которое осуществляется эксплуатационным персоналом или службой безопасности в зависимости от момента выявления нарушения, поскольку активный ненасильственный внутренний нарушитель прекращает совершение злоумышленного действия в случае противодействия или препятствования;
c) реагирование на действие активного насильственного внутреннего нарушителя, которое является таким же, как и реагирование на действие внешнего нарушителя.

4.87. Внутренний нарушитель труднее поддается выявлению по сравнению с внешним нарушителем, и его нелегко идентифицировать как угрозу в любой точке на установке. Кроме того, злоумышленный акт, совершенный внутренним нарушителем, может состоять из нескольких действий, разделенных как во времени, так и в пространстве. Поэтому, если внутренний нарушитель не может быть идентифицирован в момент выявлении подозрительного или злоумышленного действия, впоследствии его идентификация среди других сотрудников установки может быть затруднена.

4.88. В целях обеспечения эффективного реагирования на хищение, совершаемое на протяжении длительного времени, такое хищение необходимо выявлять до того, как внутренний нарушитель сможет накопить целевое количество материала на объекте или за его пределами. Следует обеспечивать, чтобы рассматриваемые сценарии охватывали системы и меры обеспечения физической безопасности, применяемые в здании и в любых возможных зонах баланса материала, а также конкретные процедуры обеспечения физической ядерной безопасности, которые могут использоваться для выявления несанкционированной деятельности, связанной с ядерным материалом, на достаточно раннем этапе, позволяющем осуществлять эффективное реагирование. В случае установок, на которых может совершаться хищение на протяжении длительного времени, следует проводить анализ сценариев для определения вероятности выявления хищения материала, когда он a) выносится/вывозится с установки каждый раз при совершении хищения некоторого количества материала или b) накапливается на установке или внутри технологической зоны для одноразового выноса/вывоза с установки в ходе реализации операции внезапного хищения.

4.89. Внутренний нарушитель может совершать ряд действий, в конечном счете направленных на несанкционированное изъятие или саботаж (диверсию) в неожиданном порядке или с периодами бездействия между отдельными действиями. Например, внутренний нарушитель может совершить одиночное действие и затем ждать для того, чтобы выяснить будет ли это действие обнаружено или нет. Это может усложнять реагирование служб обеспечения физической безопасности, необходимое для идентификации и задержания внутреннего нарушителя, и повышает роль расследования. В расследовании может требоваться помощь специалистов по эксплуатации для проведения анализа отклоняющегося от нормального или нештатного события с целью прогнозирования дальнейших злоумышленных актов, которые могут быть совершены.

4.90. Следует обеспечивать, чтобы сотрудники, имеющие доступ к установке, получали подготовку по вопросам выявления злоумышленных действий и реагирования на них, с тем чтобы они могли защитить себя и передать тревожный сигнал в соответствии с установленными процедурами. Эти процедуры следует документировать и использовать при проведении подготовки по вопросам физической безопасности, организуемой оператором для персонала установки. При разработке процедур реагирования следует исходить из допущения, что среди лиц, участвующих в осуществлении реагирования, может оказаться внутренний нарушитель. Например, внутренний нарушитель может сообщить о ложной чрезвычайной или аварийной ситуации с целью отвлечения внимания других сотрудников и создания им помех в выявлении злоумышленного действия, или же внутренний нарушитель из группы реагирования может использовать противоаварийные учения или создать чрезвычайную или аварийную ситуацию с целью маскировки злоумышленного действия.

Меры реагирования, осуществляемые применительно к компьютерным системам

4.91. Меры реагирования, осуществляемые в случае инцидентов в области компьютерной безопасности, которые могут оказать негативное воздействие на системы, связанные с обеспечением физической ядерной безопасности, следует координировать с действиями персонала, отвечающего за физическую ядерную безопасность, и документально фиксировать. Например, при обнаружении несанкционированных изменений, внесенных внутренним нарушителем в систему контроля доступа, реагирование следует осуществлять на скоординированной основе с участием персонала службы безопасности объекта и сотрудников, отвечающих за компьютерную безопасность, поскольку такие изменения могут облегчать несанкционированное изъятие или совершение акта саботажа (диверсии). В случае такого инцидента в области компьютерной безопасности следует также рассматривать целесообразность применения компенсирующих мер, предусматривающих участие службы безопасности объекта и других соответствующих подразделений установки.

КОМПЛЕКСНЫЕ ЭЛЕМЕНТЫ, УСИЛИВАЮЩИЕ ПРЕДУПРЕДИТЕЛЬНЫЕ И ЗАЩИТНЫЕ МЕРЫ

Культура физической ядерной безопасности

4.92. Культура физической ядерной безопасности основана на признании существования вероятной угрозы и важности обеспечения физической ядерной безопасности [11].

4.93. Культура физической ядерной безопасности играет ключевую роль в обеспечении поддержания бдительности лиц, организаций и учреждений, а также принятия устойчивых мер, направленных на противодействие угрозам, создаваемым внутренним нарушителем. Эффективность предупредительных и защитных мер, направленных на противодействие угрозам, создаваемым внутренним нарушителем, зависит от отношения, поведения и действий отдельных лиц [17].

4.94. Следует обеспечивать, чтобы административное руководство стимулировало формирование высокой культуры физической ядерной безопасности с целью противодействия внешним угрозам и угрозам со стороны внутреннего нарушителя. Культура физической ядерной безопасности создает общие условия для персонала, способствующие осуществлению как предупредительных, так и защитных мер. Следует обеспечивать, чтобы культура физической ядерной безопасности на установке способствовала повышению лояльности сотрудников и их приверженности политике в области физической безопасности. Например, руководству следует обращать внимание сотрудников на их обязанность сообщать о необычных действиях или подозрительном поведении, не опасаясь последующих дисциплинарных мер [11].

Планы чрезвычайных мер

4.95. Пункт 3.58 в [2] гласит:

> «Государству следует разработать и применять *план чрезвычайных мер*. *Компетентному органу* государства следует обеспечивать подготовку *оператором планов чрезвычайных мер* с целью эффективного противодействия в соответствии с *оценкой угроз* или *проектной угрозой* с учетом действий, предпринимаемых *силами реагирования*».

В пункте 3.62 в [2] указано: «*Оператору* следует начинать осуществление своего *плана чрезвычайных мер* после *обнаружения* и оценки любого *злоумышленного действия*». Пункт 5.44 в [2] гласит: «В *план чрезвычайных мер* следует включать меры, которые сосредоточены на предотвращении дальнейшего ущерба, на обеспечении физической безопасности *ядерной установки* и на защите аварийного оборудования и персонала».

4.96. В планах чрезвычайных мер, разрабатываемых государством и оператором, следует предусматривать меры реагирования как на угрозы со стороны внутреннего нарушителя, так и на внешние угрозы. В соответствии с установленным порядком защитные меры, направленные на противодействие угрозам, создаваемым внутренним нарушителем, следует координировать с планами чрезвычайных мер. Следует обеспечивать, чтобы в целях защиты от угроз со стороны внутреннего нарушителя план чрезвычайных мер предписывал проведение контроля и проверки персонала, эвакуируемого из здания во время реальной или симулируемой (учебной) аварийной или чрезвычайной ситуации, на предмет наличия радиоактивного загрязнения и ядерного материала.

4.97. Меры, принимаемые при реагировании на подозрительные или получившие подтверждение злоумышленные действия со стороны внутреннего нарушителя, могут отличаться от мер реагирования, осуществляемых в случае злоумышленного действия, совершаемого внешним нарушителем.

Программа технического обслуживания и восстановления систем

4.98. Программа технического обслуживания и восстановления, предназначенная для всех систем физической ядерной безопасности установки, защиту которых необходимо обеспечивать, позволяет смягчать последствия злоумышленного действия, совершаемого внутренним нарушителем. Программу технического обслуживания следует разрабатывать так, чтобы она обеспечивала оперативное проведение ремонта эксплуатационных и других особо важных систем, быструю замену поврежденных узлов и деталей и применение в случае необходимости компенсирующих мер. Оперативный ремонт и быстрая замена ограничивают продолжительность периода отключения системы, а также время, доступное для совершения злоумышленных действий, и позволяют смягчить последствия злоумышленного действия, совершаемого внутренним нарушителем.

4.99. Операторам следует рассматривать целесообразность обеспечения защиты мест хранения запасных частей (например, путем установки барьеров, хранения запасных частей на удалении от системы и частого проведения мониторинга места хранения), с тем чтобы затруднить внутреннему нарушителю совершение актов уничтожения или порчи как смонтированных деталей, так и запасных частей особо важного оборудования.

4.100. Следует предусматривать, чтобы эксплуатационные процедуры установки и процедуры восстановления систем физической безопасности и эксплуатационных систем проходили валидацию и отрабатывались в ходе тренировок в целях обеспечения оперативного восстановления этих систем, а также защиты аварийного оборудования и персонала.

4.101. Следует обеспечивать, чтобы процедуры, применяемые для защиты определенного оборудования, включали такие надлежащие меры реагирования на отключения или сбои в работе, как принятие компенсирующих мер, расследование причины отключения/сбоя и применение системы быстрого ремонта (возврата в рабочее состояние) с целью обеспечения защиты в случае остающегося не выявленным в результате оценки и продолжающегося злоумышленного акта.

4.102. Для чувствительных компьютерных систем, обеспечивающих выполнение эксплуатационных функций или функций физической безопасности, следует предусматривать защищенные процессы резервного копирования и восстановления. Системные файлы, используемые для процессов восстановления, следует хранить в отдельном месте, в котором предусмотрен контроль доступа.

5. ОЦЕНКА МЕР

ЦЕЛИ И ОБЗОР ПРОЦЕССА ОЦЕНКИ

5.1. Процесс оценки эффективности предупредительных и защитных мер, направленных на противодействие угрозам, создаваемым внутренним нарушителем, является ключевым компонентом оценки рисков, предназначенной для выявления систем, уязвимых для таких угроз. В этой

оценке следует использовать вероятные сценарии угроз, основанные на результатах оценки угроз или ПУ.

5.2. Результаты оценки следует сравнивать с ранее установленными критериями эффективности предупредительных и защитных мер. Эти критерии обычно устанавливаются компетентным органом с учетом потенциальных последствий злоумышленного действия, совершаемого внутренним нарушителем, и вероятности его успешного завершения. Выполнение оператором этих критериев следует документально отражать в принимаемом оператором комплексном плане обеспечения физической безопасности, включающем планы защиты как СУиК ЯМ, так и систем физической защиты.

5.3. Оценку эффективности предупредительных и защитных мер следует проводить согласно плану оператора по обеспечению физической безопасности. Если оценка указывает на то, что предупредительные и защитные меры, предусмотренные в плане обеспечения физической безопасности, не удовлетворяют установленным критериям, следует вносить необходимые изменения и повторять оценку до тех пор, пока не будет обеспечено соблюдение критериев.

5.4. При проведении оценки оператору следует учитывать относительную легкость совершения злоумышленного действия и уровень риска, связанного с потенциальным злоумышленным действием. Например, злоумышленное действие может иметь последствия, считающиеся приемлемыми, но при этом данное действие относительно легко может быть осуществлено (в частности, это может быть несанкционированное изменение порога обнаружения у радиационного портального монитора); такое действие может квалифицироваться как неприемлемое и требовать применения корректирующих мер. Риск также может считаться приемлемым, но быть близок к пороговому значению, за пределами которого он становится неприемлемым. Например, внутренний нарушитель может совершать изъятие из технологической зоны, содержащей материал категории III, небольших количеств ядерного материала, которые по отдельности создают небольшой риск, но, если это несанкционированное изъятие будет носить повторный характер, суммарный объем изъятого материала может достигнуть количества, которое должно быть отнесено к более высокой категории. Такой случай не следует исключать из рассмотрения, и в рамках практики рационального управления может предусматриваться принятие дополнительных защитных мер.

5.5. Периодически следует проводить повторные оценки эффективности предупредительных и защитных мер, в частности в случаях, когда вносятся изменения в оценку угроз или ПУ, в предупредительные и защитные меры или в эксплуатационные процессы и условия.

5.6. Критерии и требования, предусмотренные в отношении эффективности функционирования СУиК ЯМ, устанавливаются в общем контексте физической ядерной безопасности и могут быть использованы при оценке эффективности системы физической ядерной безопасности в обеспечении противодействия угрозам, создаваемым внутренним нарушителем. Эти критерии и требования по обеспечению эффективности функционирования следует применять в отношении различных типов ядерного материала и сроков выявления несанкционированного изъятия ядерного материала.

5.7. Для оценки эффективности системы физической ядерной безопасности в обеспечении противодействия угрозам, создаваемым внутренним нарушителем, могут использоваться различные методы (например, инспекции и оценки, тестирование эффективности функционирования, контроль качества измерений, анализ сценариев). Анализ сценариев — это эффективный метод оценки противодействия угрозам, создаваемым внутренним нарушителем. Тестирование эффективности функционирования служит инструментом, помогающим проводить анализ сценариев благодаря получению, в частности, информации о вероятности выявления и о последующем реагировании. Следует разрабатывать и вводить в действие планы тестирования эффективности функционирования для проверки готовности сотрудников, установки и компетентных органов к реагированию в случае потенциального злоумышленного действия со стороны внутреннего нарушителя.

ОЦЕНКА ПРЕДУПРЕДИТЕЛЬНЫХ МЕР

5.8. Применение предупредительных мер следует оценивать с целью обеспечить их осуществление так, как это было предусмотрено. Предупредительные меры трудно поддаются количественной оценке, однако они могут быть эффективными в снижении вероятности угроз со стороны внутреннего нарушителя. Предупредительные меры следует оценивать путем тестирования эффективности функционирования применяемых процедур, позволяющего определить, являются ли данные процедуры адекватными для целей противодействия угрозам и соблюдают ли сотрудники эти процедуры.

5.9. Возможности совершения внутренним нарушителем злоумышленного действия могут быть сведены к минимуму за счет ограничения возможности получения внутренним нарушителем доступа, полномочий или знаний, необходимых для успешного совершения злоумышленного действия. Вероятные сценарии, используемые при проведении оценки, предполагают определение степени и способов сведения такой возможности к минимуму. Следует проводить анализ, позволяющий проверить, какие предупредительные меры приняты и правильно ли они применяются.

ОЦЕНКА ЗАЩИТНЫХ МЕР

5.10. Эффективность мер, используемых для выявления, задержки осуществления злоумышленных действий и реагирования на них (т.е. защитных мер), поддается количественному или качественному анализу. Вероятность выявления и своевременность реагирования во многих случаях поддаются количественной оценке и могут служить основой для оценки эффективности защитных мер.

5.11. Один из методов оценки эффективности защитных мер, направленных на противодействие угрозам, создаваемым внутренним нарушителем, заключается в разработке и анализе вероятных сценариев, в том числе сценариев сговора с другими внутренними нарушителями или с внешними нарушителями, в зависимости от конкретных обстоятельств. Затем может быть проведена оценка эффективности защитных мер в обеспечении противодействия этим сценариям.

5.12. Разработка и анализ сценариев предполагает определение сочетания действий, необходимых внутреннему нарушителю для совершения злоумышленного акта. При разработке сценариев операторам следует рассматривать возможность привязки идентифицированных целей (см. раздел 3) к определенным внутренним нарушителям (см. раздел 2). Совокупность действий, которые потребуется совершить внутреннему нарушителю для достижения своей цели, следует определять с учетом оценки угроз или ПУ. Следует обеспечивать, чтобы эта совокупность действий отражала совершаемые действия и места, где они будут осуществляться, а также все защитные меры, с которыми могут столкнуться внутренние нарушители при совершении этих действий. Ввиду того, что внутренние нарушители могут осуществлять действия, необходимые для совершения злоумышленного акта, в течение длительного времени, и поскольку эти действия могут не соответствовать прогнозируемой последовательности,

концепция пути или временной шкалы действий не всегда подходит для целей анализа.

5.13. При анализе сценариев саботажа (диверсии) следует определять действия, которые необходимо осуществить для инициирования последовательности событий, могущих привести к неприемлемым радиологическим последствиям. В сценарии саботажа следует включать атаки как на одиночные, так и на множественные цели.

5.14. При разработке сценариев с несанкционированным изъятием ядерного материала следует определять действия, которые необходимо успешно осуществить для изъятия ядерного материала из установки. В сценариях с несанкционированным изъятием ядерного материала следует предусматривать случаи как хищения на протяжении длительного времени, так и внезапного хищения, а также ситуации, в которых внутренний нарушитель покидает установку непосредственно с ядерным материалом или прячет материал на установке для того, чтобы впоследствии изъять его из установки при более благоприятных для него обстоятельствах. В сценариях следует учитывать атаки или компрометацию (взлом) компьютерных систем, сочетание физических атак и кибератак, а также атаки, совершаемые насильственными и ненасильственными внутренними нарушителями.

5.15. При разработке и анализе сценария следует рассматривать также стратегии, которые внутренние нарушители могут использовать для преодоления защитных мер. Оператор может моделировать такие стратегии путем анализа того, как внутренний нарушитель может использовать полученные им доступ, полномочия и знания для блокирования мер выявления и мер задержки осуществления. Следует также учитывать возможные попытки внутренних нарушителей снизить эффективность реагирования. Аварийные условия, приводящие к эвакуации людей с установки, могут создавать возможности для совершения внутренним нарушителем злоумышленного действия, и такие условия следует учитывать при проработке сценариев.

5.16. По окончании разработки детальных сценариев, связанных с противодействием угрозам, создаваемым внутренним нарушителем, может быть проведена оценка эффективности защитных мер путем анализа суммарного эффекта, обеспечиваемого средствами выявления и задержки осуществления, а также мер по реагированию и смягчению последствий, возникающих в случае данного сценария. Эффективность мер реагирования

в случае активного ненасильственного внутреннего нарушителя зависит от вероятности блокирования или нейтрализации[5] злоумышленного действия.

5.17. Процесс оценки следует повторять применительно к вероятным сценариям, в случае которых требуется проведение дополнительного анализа. Выводы об эффективности защитных мер следует основывать на результатах всех проведенных оценок.

ОЦЕНКА МЕР, НАПРАВЛЕННЫХ НА ПРОТИВОДЕЙСТВИЕ СГОВОРУ МЕЖДУ ВНУТРЕННИМИ НАРУШИТЕЛЯМИ

5.18. Разработка достаточного набора сценариев, предусматривающих противодействие сговору между двумя или большим числом внутренних нарушителей, представляет собой сложную задачу из-за многочисленности комбинаций участия внутренних нарушителей с разными уровнями доступа, полномочий и знаний, которые необходимо учитывать. Хорошим подходом в такой ситуации может быть оценка эффективности мер, предназначенных для предупреждения сговора (например, мер по разделению видов работ, наблюдению, а также предупредительных мер).

ОЦЕНКА МЕР, НАПРАВЛЕННЫХ НА ПРОТИВОДЕЙСТВИЕ ХИЩЕНИЮ, СОВЕРШАЕМОМУ НА ПРОТЯЖЕНИИ ДЛИТЕЛЬНОГО ВРЕМЕНИ

5.19. К оценке мер, направленных на противодействие хищению, совершаемому на протяжении длительного времени, можно подходить так же, как к оценке мер, направленных на противодействие внезапному хищению. В то же время при оценке мер, направленных на противодействие хищению, совершаемому на протяжении длительного времени, следует также учитывать дополнительные трудности, с которыми сталкивается внутренний нарушитель при попытке совершать несанкционированное изъятие малых количеств материала в течение продолжительного

---

[5] Под «блокированием» подразумевается осуществление своевременного реагирования, обеспечивающего предупреждение завершения злоумышленного действия. В случае активного насильственного внутреннего нарушителя «нейтрализация» означает, что силы реагирования полностью останавливают или предотвращают атаку. Применительно к активному, ненасильственному внутреннему нарушителю нейтрализация осуществляется в момент идентификации нарушителя.

интервала времени. Эти трудности обусловлены, в частности, проведением периодических проверок инвентарного количества материала, возможным обнаружением расхождений в данных об инвентарных количествах, обеспечением отслеживания регистрационных записей, засекречиванием сведений о накопленном количестве материала и контролем с применением радиационных портальных мониторов. При применении данного метода оценки также следует учитывать то, что вероятность выявления нарушения повышается в случае неоднократного повторения одного и того же действия.

ОЦЕНКА МЕР, НАПРАВЛЕННЫХ НА ПРОТИВОДЕЙСТВИЕ САБОТАЖУ

5.20. При проведении оценки мер, направленных на противодействие саботажу (диверсии), совершаемому внутренним нарушителем, можно использовать процесс, применяемый при оценке мер, направленных на противодействие внезапному хищению и хищению, осуществляемому на протяжении длительного времени, и для этой оценки может использоваться подход, основанный на логической модели (дереве отказов или дереве событий), как указано в [16].

5.21. В число сценариев саботажа, подлежащих оценке, следует включать сценарии как прямого саботажа в отношении ядерного материала, так и косвенного саботажа (т.е. актов саботажа в отношении систем установки), которые могут привести к неприемлемым радиологическим последствиям. При оценке сценариев саботажа следует также рассматривать сценарии действий лиц, не имеющих прямого доступа к материалу или оборудованию.

5.22. При совершении акта саботажа внутренний нарушитель не обязательно должен покидать установку для осуществления злоумышленного действия. Поэтому в этом случае применяется оценка предупредительных и защитных мер, направленных на противодействие любому внутреннему нарушителю, покидающему пределы установки.

ОЦЕНКА УСТАНОВКИ НА ПРЕДМЕТ ОБЕСПЕЧЕНИЯ ЗАЩИТЫ ОТ УГРОЗ, СОЗДАВАЕМЫХ ВНУТРЕННИМ НАРУШИТЕЛЕМ

5.23. Процесс оценки установки на предмет обеспечения защиты от угроз, создаваемых внутренним нарушителем, начинается с характеризации внутренних нарушителей по атрибутивным признакам, мотивации

и категориям для идентификации потенциальных угроз со стороны внутреннего нарушителя. Следующим шагом является идентификация целей, включающая оценку активов, защиту которых от несанкционированного изъятия или саботажа необходимо обеспечивать. Результатом этой оценки является приоритизированный перечень целей.

5.24. Для сведения к минимуму возможности реализации идентифицированных угроз и целей, являющихся предметом злоумышленных действий, при осуществлении предупредительных мер следует применять концепцию глубокоэшелонированной защиты и дифференцированный подход.

5.25. В приоритетном порядке следует определять защитные меры, обеспечивающие защиту целей в защищенных, внутренних или особо важных зонах. На основе результатов оценки следует при необходимости увеличивать глубину защиты, обеспечиваемую мерами по выявлению, задержке осуществления и реагированию, применительно к угрозам, создаваемым внутренним нарушителем.

5.26. Предупредительные и защитные меры, направленные на противодействие саботажу и несанкционированному изъятию ядерного материала, следует оценивать с использованием таких методов, как разработка и анализ вероятных сценариев. Следует обеспечивать, чтобы сценарии соответствовали оценке угроз или ПУ и по возможности включали физические атаки, кибератаки или их сочетание, совершаемые на установке, во время транспортировки и в цепочках поставок.

5.27. Оценку системы следует периодически пересматривать в целях обеспечения эффективного и устойчивого применения предупредительных и защитных мер. Повторные оценки могут проводиться на регулярной основе, а также внепланово при изменении угрозы или введении изменений на установке и в ее эксплуатацию.

СПРАВОЧНЫЕ МАТЕРИАЛЫ

[1] МЕЖДУНАРОДНОЕ АГЕНТСТВО ПО АТОМНОЙ ЭНЕРГИИ, «Цель и основные элементы государственного режима физической ядерной безопасности», Серия изданий МАГАТЭ по физической ядерной безопасности, № 20, МАГАТЭ, Вена (2014).

[2] МЕЖДУНАРОДНОЕ АГЕНТСТВО ПО АТОМНОЙ ЭНЕРГИИ, «Рекомендации по физической ядерной безопасности, касающиеся физической защиты ядерных материалов и ядерных установок» (INFCIRC/225/Revision 5), Серия изданий МАГАТЭ по физической ядерной безопасности, № 13, МАГАТЭ, Вена (2012).

[3] МЕЖДУНАРОДНОЕ АГЕНТСТВО ПО АТОМНОЙ ЭНЕРГИИ, «Рекомендации по физической ядерной безопасности, касающиеся радиоактивных материалов и связанных с ними установок», Серия изданий МАГАТЭ по физической ядерной безопасности, № 14, МАГАТЭ, Вена (2011).

[4] 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, Всемирная таможенная организация, «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).

[5] INTERNATIONAL ATOMIC ENERGY AGENCY, Security of Radioactive Sources, IAEA Nuclear Security Series No. 11, IAEA, Vienna (2009).

[6] INTERNATIONAL ATOMIC ENERGY AGENCY, Security in the Transport of Radioactive Material, IAEA Nuclear Security Series No. 9, IAEA, Vienna (2008).

[7] МЕЖДУНАРОДНОЕ АГЕНТСТВО ПО АТОМНОЙ ЭНЕРГИИ, «Компьютерная безопасность на ядерных установках», № 17, МАГАТЭ, Вена (2012).

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

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

[10] 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).

[11] МЕЖДУНАРОДНОЕ АГЕНТСТВО ПО АТОМНОЙ ЭНЕРГИИ, Культура физической ядерной безопасности Серия изданий МАГАТЭ по физической ядерной безопасности, № 7, МАГАТЭ, Вена (2022).

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

[13] INTERNATIONAL ATOMIC ENERGY AGENCY, Security of Nuclear Material in Transport, IAEA Nuclear Security Series No. 26G, IAEA, Vienna (2015).
[14] INTERNATIONAL ATOMIC ENERGY AGENCY, Establishing a System for Control of Nuclear Material for Nuclear Security Purposes at a Facility during Use, Storage and Movement, IAEA Nuclear Security Series No. 32T, IAEA, Vienna (2019).
[15] INTERNATIONAL ATOMIC ENERGY AGENCY, Physical Protection of Nuclear Material and Nuclear Facilities (Implementation of INFCIRC/225/Revision 5), IAEA Nuclear Security Series No. 27G, IAEA, Vienna (2018).
[16] INTERNATIONAL ATOMIC ENERGY AGENCY, Identification of Vital Areas at Nuclear Facilities, IAEA Nuclear Security Series No. 16, IAEA, Vienna (2012).
[17] INTERNATIONAL ATOMIC ENERGY AGENCY, Selfassessment of Nuclear Security Culture in Facilities and Activities, IAEA Nuclear Security Series No. 28T, IAEA, Vienna (2007).

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 представляет собой обновленное издание публикации в Серии изданий МАГАТЭ по физической ядерной безопасности, № 8, опубликованной в 2008 году (в 2009 году на русском языке). Цели пересмотра сводились к тому, чтобы обеспечить более полную согласованность настоящего Практического руководства с публикацией «Основы физической ядерной безопасности» и с рекомендациями по физической ядерной безопасности, опубликованными после 2008 года, включить ссылки на другие практические руководства, опубликованные после 2008 года, а также добавить дополнительную детальную информацию по некоторым вопросам, учитывающую опыт МАГАТЭ и государств-членов, накопленный в использовании публикации Серии изданий МАГАТЭ по физической ядерной безопасности, № 8. В настоящей публикации изложены обновленные рекомендации, предназначенные для государств, их компетентных органов и операторов, а также грузоотправителей и перевозчиков, по выбору, реализации и оценке мер, направленных на противодействие угрозам, создаваемым внутренними нарушителями (иногда называемыми «инсайдерами»). Руководство применимо к любому типу ядерных установок, в частности, к атомным электростанциям, исследовательским реакторам и другим установкам ядерного топливного цикла (например, заводам по обогащению, заводам по переработке, заводам по изготовлению топлива, хранилищам), находящимся на стадиях проектирования, строительства, ввода в эксплуатацию, эксплуатации, остановки или вывода из эксплуатации.

МЕЖДУНАРОДНОЕ АГЕНТСТВО ПО АТОМНОЙ ЭНЕРГИИ
ВЕНА