Серия изданий МАГАТЭ по физической ядерной безопасности, № 8

Настоящая публикация была заменена публикацией No. 8-G (Rev. 1).

Практическое руководство

Предупредительные и защитные меры в отношении угроз, исходящих от внутреннего нарушителя

IAEA
Международное агентство по атомной энергии

Настоящая публикация была заменена публикацией No. 8-G (Rev. 1).

СЕРИЯ ИЗДАНИЙ МАГАТЭ ПО ФИЗИЧЕСКОЙ ЯДЕРНОЙ БЕЗОПАСНОСТИ

В публикациях **Серии изданий МАГАТЭ по физической ядерной безопасности** рассматриваются вопросы физической ядерной безопасности, касающиеся предотвращения и обнаружения хищения, саботажа, несанкционированного доступа, незаконной передачи или других злоумышленных действий в отношении ядерного материала, других радиоактивных веществ или связанных с ними установок и реагирования на такие действия. Эти публикации соответствуют таким международным договорно-правовым документам в области физической ядерной безопасности, как Конвенция о физической защите ядерного материала с внесенными в нее поправками, Кодекс поведения по обеспечению безопасности и сохранности радиоактивных источников, резолюции 1373 и 1540 Совета Безопасности Организации Объединенных Наций и Международная конвенция о борьбе с актами ядерного терроризма, а также дополняют их.

КАТЕГОРИИ ПУБЛИКАЦИЙ В СЕРИИ ИЗДАНИЙ МАГАТЭ ПО ФИЗИЧЕСКОЙ ЯДЕРНОЙ БЕЗОПАСНОСТИ

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

- **"Основы физической ядерной безопасности"**, которые содержат задачи, концепции и принципы физической ядерной безопасности и на основе которых составляются рекомендации в отношении физической безопасности.
- **"Рекомендации"**, где излагается передовой опыт, который следует использовать государствам-членам при осуществлении "Основ физической ядерной безопасности".
- **"Практические руководства"**, в которых развиваются рекомендации по широким направлениям деятельности и предлагаются меры по их осуществлению.
- Публикации, относящиеся к **"Техническим руководящим материалам"**, включают: **"Справочные руководства"**, в которых подробно описываются меры и/или даются руководящие указания в отношении применения практических руководств в конкретных областях или видах деятельности; **"Учебные руководства"**, касающиеся учебных планов и/или учебных пособий для учебных курсов МАГАТЭ в области физической ядерной безопасности; **"Руководства по услугам"**, в которых даются руководящие указания в отношении проведения и масштабов консультативных миссий МАГАТЭ по физической ядерной безопасности.

ПОДГОТОВКА И РАССМОТРЕНИЕ

В подготовке этих публикаций Секретариату МАГАТЭ помогают международные эксперты. В отношении документов категорий "Основы физической ядерной безопасности", "Рекомендации" и "Практические руководства" МАГАТЭ проводит технические совещания открытого состава, чтобы заинтересованные государства-члены и соответствующие международные организации имели надлежащую возможность рассмотреть проект текста. Кроме того, для обеспечения высокого уровня международного рассмотрения и достижения консенсуса Секретариат представляет проекты текстов всем государствам-членам на период в 120 дней на официальное рассмотрение. Это дает возможность государствам-членам в полной мере выразить свое мнение до опубликования текста.

Публикации категории "Технические руководящие материалы" готовятся в тесных консультациях с международными экспертами. Проведение технических совещаний не требуется, но они могут быть при необходимости организованы для ознакомления с широким спектром мнений.

В процессе подготовки и рассмотрения публикаций Серии МАГАТЭ по физической ядерной безопасности учитываются соображения конфиденциальности и признается, что вопросы физической ядерной безопасности неразрывно связаны с общими и конкретными задачами национальной безопасности. Одним их основополагающих факторов является необходимость учета в техническом содержании публикаций соответствующих норм безопасности МАГАТЭ и деятельности по гарантиям.

Настоящая публикация была заменена публикацией No. 8-G (Rev. 1).

ПРЕДУПРЕДИТЕЛЬНЫЕ И ЗАЩИТНЫЕ МЕРЫ В ОТНОШЕНИИ УГРОЗ, ИСХОДЯЩИХ ОТ ВНУТРЕННЕГО НАРУШИТЕЛЯ

Настоящая публикация была заменена публикацией No. 8-G (Rev. 1).

Членами Международного агентства по атомной энергии являются следующие государства:

АВСТРАЛИЯ
АВСТРИЯ
АЗЕРБАЙДЖАН
АЛБАНИЯ
АЛЖИР
АНГОЛА
АРГЕНТИНА
АРМЕНИЯ
АФГАНИСТАН
БАНГЛАДЕШ
БАХРЕЙН
БЕЛАРУСЬ
БЕЛЬГИЯ
БЕЛИЗ
БЕНИН
БОЛГАРИЯ
БОЛИВИЯ
БОСНИЯ И ГЕРЦЕГОВИНА
БОТСВАНА
БРАЗИЛИЯ
БУРКИНА-ФАСО
БУРУНДИ
БЫВШАЯ ЮГОСЛ. РЕСП. МАКЕДОНИЯ
ВЕНГРИЯ
ВЕНЕСУЭЛА
ВЬЕТНАМ
ГАБОН
ГАИТИ
ГАНА
ГВАТЕМАЛА
ГЕРМАНИЯ
ГОНДУРАС
ГРЕЦИЯ
ГРУЗИЯ
ДАНИЯ
ДЕМОКРАТИЧЕСКАЯ РЕСПУБЛИКА КОНГО
ДОМИНИКАНСКАЯ РЕСПУБЛИКА
ЕГИПЕТ
ЗАМБИЯ
ЗИМБАБВЕ
ИЗРАИЛЬ
ИНДИЯ
ИНДОНЕЗИЯ
ИОРДАНИЯ
ИРАК
ИРАН, ИСЛАМСКАЯ РЕСПУБЛИКА
ИРЛАНДИЯ
ИСЛАНДИЯ
ИСПАНИЯ
ИТАЛИЯ
ЙЕМЕН
КАЗАХСТАН
КАМЕРУН
КАНАДА
КАТАР
КЕНИЯ
КИПР
КИТАЙ
КОЛУМБИЯ
КОРЕЯ, РЕСПУБЛИКА
КОСТА-РИКА
КОНГО
КОТ-Д'ИВУАР
КУБА
КУВЕЙТ
КЫРГЫЗСТАН
ЛАТВИЯ
ЛИБЕРИЯ
ЛИВАН
ЛИВИЙСКАЯ АРАБСКАЯ ДЖАМАХИРИЯ
ЛИТВА
ЛИХТЕНШТЕЙН
ЛЮКСЕМБУРГ
ЛЕСОТО
МАВРИКИЙ
МАВРИТАНИЯ
МАДАГАСКАР
МАЛАВИ
МАЛАЙЗИЯ
МАЛИ
МАЛЬТА
МАРОККО
МАРШАЛЛОВЫ ОСТРОВА
МЕКСИКА
МОНАКО
МОНГОЛИЯ
МОЗАМБИК
МЬЯНМА
НАМИБИЯ
НЕПАЛ
НИГЕР
НИГЕРИЯ
НИДЕРЛАНДЫ
НИКАРАГУА
НОВАЯ ЗЕЛАНДИЯ
НОРВЕГИЯ
ОБЪЕДИНЕННАЯ РЕСПУБЛИКА ТАНЗАНИЯ
ОБЪЕДИНЕННЫЕ АРАБСКИЕ ЭМИРАТЫ
ОМАН
ПАКИСТАН
ПАЛАУ
ПАНАМА
ПАРАГВАЙ
ПЕРУ
ПОЛЬША
ПОРТУГАЛИЯ
РЕСПУБЛИКА МОЛДОВА
РОССИЙСКАЯ ФЕДЕРАЦИЯ
РУМЫНИЯ
САЛЬВАДОР
САУДОВСКАЯ АРАВИЯ
СЕЙШЕЛЬСКИЕ ОСТРОВА
СВЯТЕЙШИЙ ПРЕСТОЛ
СЕНЕГАЛ
СЕРБИЯ
СИНГАПУР
СИРИЙСКАЯ АРАБСКАЯ РЕСПУБЛИКА
СЛОВАКИЯ
СЛОВЕНИЯ
СОЕДИНЕННОЕ КОРОЛЕВСТВО ВЕЛИКОБРИТАНИИ И СЕВЕРНОЙ ИРЛАНДИИ
СОЕДИНЕННЫЕ ШТАТЫ АМЕРИКИ
СУДАН
СЬЕРРА-ЛЕОНЕ
ТАДЖИКИСТАН
ТАИЛАНД
ТУНИС
ТУРЦИЯ
УГАНДА
УЗБЕКИСТАН
УКРАИНА
УРУГВАЙ
ФИЛИППИНЫ
ФИНЛЯНДИЯ
ФРАНЦИЯ
ХОРВАТИЯ
ЦЕНТРАЛЬНОАФРИКАНСКАЯ РЕСПУБЛИКА
ЧАД
ЧЕРНОГОРИЯ
ЧЕШСКАЯ РЕСПУБЛИКА
ЧИЛИ
ШВЕЙЦАРИЯ
ШВЕЦИЯ
ШРИ-ЛАНКА
ЭКВАДОР
ЭРИТРЕЯ
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”.

Настоящая публикация была заменена публикацией No. 8-G (Rev. 1).

СЕРИЯ ИЗДАНИЙ МАГАТЭ ПО ФИЗИЧЕСКОЙ ЯДЕРНОЙ БЕЗОПАСНОСТИ, № 8

ПРЕДУПРЕДИТЕЛЬНЫЕ И ЗАЩИТНЫЕ МЕРЫ В ОТНОШЕНИИ УГРОЗ, ИСХОДЯЩИХ ОТ ВНУТРЕННЕГО НАРУШИТЕЛЯ

ПРАКТИЧЕСКОЕ РУКОВОДСТВО

МЕЖДУНАРОДНОЕ АГЕНТСТВО ПО АТОМНОЙ ЭНЕРГИИ
ВЕНА, 2009 ГОД

Настоящая публикация была заменена публикацией No. 8-G (Rev. 1).

УВЕДОМЛЕНИЕ ОБ АВТОРСКОМ ПРАВЕ

Все научные и технические публикации МАГАТЭ защищены в соответствии с положениями Всемирной конвенции об авторском праве в том виде, как она была принята в 1952 году (Берн) и пересмотрена в 1972 году (Париж). Впоследствии авторские права были распространены Всемирной организацией интеллектуальной собственности (Женева) также на интеллектуальную собственность в электронной и виртуальной форме. Для полного или частичного использования текстов, содержащихся в печатных или электронных публикациях МАГАТЭ, должно быть получено разрешение, которое обычно является предметом соглашений о роялти. Предложения о некоммерческом воспроизведении и переводе приветствуются и рассматриваются в каждом отдельном случае. Вопросы следует направлять в Издательскую секцию МАГАТЭ по адресу:

Группа продажи и рекламы
Издательская секция
Международное агентство по атомной энергии
Vienna International Centre
PO Box 100
1400 Vienna, Austria
факс: +43 1 2600 29302
тел.: +43 1 2600 22417
эл. почта: sales.publications@iaea.org
веб-сайт: http://www.iaea.org/books

© МАГАТЭ, 2009

Напечатано МАГАТЭ в Австрии
Ноябрь 2009

ПРЕДУПРЕДИТЕЛЬНЫЕ И ЗАЩИТНЫЕ МЕРЫ В ОТНОШЕНИИ УГРОЗ, ИСХОДЯЩИХ ОТ ВНУТРЕННЕГО НАРУШИТЕЛЯ

МАГАТЭ, ВЕНА, 2009
STI/PUB/1359
ISBN 978–92–0–411709–7
ISSN 1816–9317

Настоящая публикация была заменена публикацией No. 8-G (Rev. 1).

ПРЕДИСЛОВИЕ

Во исполнение резолюции GC(46)/RES/13 Генеральной конференции МАГАТЭ от 20 сентября 2002 года МАГАТЭ приняло комплексный подход к вопросам защиты от ядерного терроризма. Этот подход обеспечивает координацию деятельности МАГАТЭ в отношении физической защиты ядерного материала и ядерных установок, учета ядерного материала, обнаружения незаконного оборота ядерных и других радиоактивных материалов и реагирования на него, сохранности радиоактивных источников, физической безопасности при перевозке ядерных и других радиоактивных материалов, аварийного реагирования и аварийной готовности в государствах-членах и МАГАТЭ, а также содействия присоединению государств к соответствующим международным договорно-правовым документам и их осуществлению. МАГАТЭ помогает также определять угрозы и уязвимые места, связанные с сохранностью ядерных и других радиоактивных материалов. Однако, ответственность за физическую защиту ядерных и других радиоактивных материалов и связанных с ними установок, за обеспечение физической безопасности таких материалов при перевозке и за борьбу с незаконным оборотом и непреднамеренным перемещением радиоактивных материалов возлагается на государства.

Системы физической защиты предназначены для предотвращения неприемлемых последствий, возникающих в результате злоумышленных действий. Чем серьезнее возможные последствия, тем важнее обеспечить высокую степень уверенности в том, что системы физической защиты будут эффективно функционировать, как запланировано.

Совершение злоумышленных действий в отношении ядерного материала и ядерных установок может привести к целому ряду неприемлемых радиологических последствий и последствий с точки зрения распространения. Необходимость обеспечения высокой степени уверенности в эффективности физической защиты давно признается теми, кто имеет отношение к ядерному материалу и ядерным установкам. Для достижения наиболее высокого уровня уверенности в физической защите требуется обеспечение тесной корреляции между защитными мерами и угрозой. Этот подход твердо базируется на основополагающем принципе, который заключается в том, что физическая защита ядерных ресурсов, находящихся под юрисдикцией государства, должна основываться на проведенной государством оценке угрозы этим ресурсам.

Если иметь четкое представление об угрозе, то можно дать подробное описание возможных нарушителей, включая "внешних нарушителей" и "внутренних нарушителей".

Угрозы, исходящие от внутренних нарушителей, создают проблему для систем физической защиты, которая радикально отличается от других проблем.

Настоящая публикация была заменена публикацией No. 8-G (Rev. 1).

Внутренние нарушители могут использовать преимущество наличия у них прав доступа, дополненных их полномочиями и знанием установки, для обхода специальных элементов физической защиты или других предусмотренных мер, таких, как меры по обеспечению безопасности, контроля и учета материала, а также эксплуатационные меры и процедуры. Кроме того, являясь сотрудниками, обладающими соответствующим доступом и пользующимися доверием в соответствии со своей должностью, внутренние нарушители имеют возможности для применения методов "нанесения ущерба", которыми не располагают внешние нарушители в случае, когда им приходится сталкиваться с элементами защиты и мерами контроля доступа. Внутренние нарушители имеют больше возможностей для выбора наиболее уязвимой цели и наиболее выгодного времени для совершения злоумышленного действия.

Вопросам физической защиты от несанкционированного изъятия ядерного материала и от саботажа в отношении ядерного материала и ядерных установок посвящен целый ряд публикаций МАГАТЭ. В этих публикациях даются общие рекомендации по проектированию и оценке защитных мер, и они в основном ориентированы на предупреждение внешних угроз.

В соответствии с поставленной задачей разработки полного свода руководящих материалов было принято решение разработать руководство, конкретно посвященное теме внутренних нарушителей. В результате в настоящую публикацию были включены общие руководящие материалы по предотвращению внутренних угроз и защите от них. Она содержит руководящие материалы по выполнению рекомендаций, изложенных в документе INFCIRC/225/Rev.4 (Corrected), и пользоваться ею следует вместе с документами IAEA-TECDOC-967 (Rev.1) и IAEA-TECDOC-1276, а также другими публикациями в Серии изданий МАГАТЭ по физической ядерной безопасности.

РЕДАКЦИОННОЕ ПРИМЕЧАНИЕ

Настоящий документ не затрагивает вопросов ответственности - юридической или иного рода - за действия или бездействия со стороны какого-либо лица.

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

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

Упоминание названий конкретных компаний или продуктов (независимо от того, были они зарегистрированы или нет) не подразумевает какого-либо намерения нарушить права собственности, и его не следует рассмаривать как одобрение или рекомендацию со стороны МАГАТЭ.

Настоящая публикация была заменена публикацией No. 8-G (Rev. 1).

СОДЕРЖАНИЕ

1. ВВЕДЕНИЕ 1

1.1. Общие сведения 1
1.2. Вопросы, связанные с внутренним нарушителем 2
1.3. Цель и сфера применения 3

2. ОПРЕДЕЛЕНИЕ УГРОЗ, ИСХОДЯЩИХ ОТ ПОТЕНЦИАЛЬНЫХ ВНУТРЕННИХ НАРУШИТЕЛЕЙ 4

3. СИТУАЦИИ, КОТОРЫЕ СЛЕДУЕТ УЧИТЫВАТЬ ПРИ АНАЛИЗЕ УГРОЗ, ИСХОДЯЩИХ ОТ ВНУТРЕННИХ НАРУШИТЕЛЕЙ 7

4. ОПРЕДЕЛЕНИЕ ЦЕЛЕЙ 8

4.1. Общий обзор 8
4.2. Цели саботажа 9
4.3. Цели, которые могут стать предметом несанкционированного изъятия 10

5. МЕРЫ В ОТНОШЕНИИ ВОЗМОЖНЫХ ВНУТРЕННИХ НАРУШИТЕЛЕЙ 11

5.1. Общий подход 11
5.2. Разработка всеобъемлющего подхода 12
5.3. Предупредительные меры 14
5.4. Защитные меры 18
5.4.1. Выявление 19
5.4.2. Задержка действий 24
5.4.3. Реагирование 25
5.4.4. Планы аварийных мероприятий 26

6. ОЦЕНКА ПРЕДОХРАНИТЕЛЬНЫХ И ЗАЩИТНЫХ МЕР 27

6.1. Цели и общий обзор процесса оценки 27
6.2. Оценка предупредительных мер 29
6.3. Оценка защитных мер 29

СПРАВОЧНЫЕ МАТЕРИАЛЫ 33

Настоящая публикация была заменена публикацией No. 8-G (Rev. 1).

Настоящая публикация была заменена публикацией No. 8-G (Rev. 1).

1. ВВЕДЕНИЕ

1.1. ОБЩИЕ СВЕДЕНИЯ

Ряд публикаций МАГАТЭ посвящен вопросам физической защиты от несанкционированного изъятия ядерного материала и от саботажа в отношении ядерного материала и ядерных установок.

В Конвенции о физической защите ядерного материала (КФЗЯМ) [1] предусматриваются общие требования в отношении физической защиты ядерного материала и конкретные требования в отношении защиты материала в процессе международной перевозки. Поправка к КФЗЯМ [2] была принята на Дипломатической конференции государств - участников КФЗЯМ консенсусом 8 июля 2005 года и подлежит ратификации, принятию или одобрению. Сфера действия Поправки охватывает требования в отношении физической защиты ядерного материала при использовании, хранении и перевозке внутри государства, а также защиты ядерного материала и установок от саботажа. Кроме того, в Поправке нашли отражение "Цели и основополагающие принципы физической защиты" [3].

Документ "Цели и основополагающие принципы физической защиты" (GOV/2001/41) [3] содержит четыре общих цели и 12 принципов, которые имеют весьма важное значение для разработки всеобъемлющего режима физической защиты.

В документе "Физическая защита ядерного материала и ядерных установок", INFCIRC/225/Rev.4 (Corrected) [4], приводятся рекомендации и дополнительные руководящие материалы для компетентного органа государства в отношении порядка выполнения внутригосударственных требований таким образом, чтобы это соответствовало данным рекомендациям. Его дополняет документ IAEA-TECDOC-967 (Rev.1) "Руководящие материалы и соображения по осуществлению документа INFCIRC/225/Rev.4 (Corrected) [5].

В "Руководстве по физической защите ядерного материала и ядерных установок", IAEA-TECDOC-1276 [6], оператору установки даются практические рекомендации в отношении проектирования системы физической защиты, целого ряда мер и оборудования для той или иной конкретной установки, функций реагирования, а также руководящие указания по оценке эффективности существующей на установке системы физической защиты; внутренние угрозы, однако, охвачены этим руководством лишь ограниченно.

Настоящая публикация была заменена публикацией No. 8-G (Rev. 1).

1.2. ВОПРОСЫ, СВЯЗАННЫЕ С ВНУТРЕННИМ НАРУШИТЕЛЕМ

Термин "нарушитель" используется для описания любого лица, совершающего или пытающегося совершить злоумышленное действие (злоумышленную акцию). Нарушитель может быть внутренним или внешним. Термин "внутренний нарушитель" используется для описания нарушителя с санкционированным доступом к ядерной установке, операции по перевозке или чувствительной информации. Термин "внешний нарушитель" используется для описания нарушителя, не являющегося внутренним нарушителем.

Система физической защиты проектируется и оценивается на предмет угроз, исходящих как от внешних нарушителей, так и от внутренних нарушителей. Угрозы, исходящие от внутренних нарушителей, создают проблему, которая кардинально отличается от других проблем. Внутренние нарушители могут использовать преимущество имеющегося у них доступа (т.е. права или возможности получения разрешения на вход в данную зону), дополненного предоставленными им полномочиями (т.е. властью или правом требовать повиновения) и знанием установки (т.е. информированностью или осведомленностью в результате получения соответствующей подготовки или накопления соответствующего опыта), для обхода специальных элементов физической защиты или других предусмотренных мер, таких, как обеспечение безопасности, контроль и учет ядерного материала (КиУМ), а также эксплуатационные меры и процедуры.

Кроме того, являясь сотрудниками, имеющими санкционированный доступ и пользующимися доверием в соответствии со своей должностью, внутренние нарушители имеют возможности для применения методов нанесения ущерба, которыми не располагают внешние нарушители. Внутренние нарушители имеют больше возможностей (т.е. находятся в более благоприятных условиях) для выбора наиболее уязвимой цели и наиболее выгодного времени для совершения или попытки совершения злоумышленного действия. Для того, чтобы в максимально возможной степени обеспечить вероятность успеха, они могут растягивать процесс исполнения злоумышленной акции и осуществлять его в течение длительного времени. Этот процесс может включать, например, вмешательство в обеспечивающее безопасность оборудование для подготовки к попытке совершения акта саботажа или к совершению этого акта, или же фальсификацию материально-балансовых учетных документов с целью неоднократного хищения небольших количеств ядерного материала.

Настоящее руководство содержит руководящие материалы по выполнению рекомендаций, изложенных в документе INFCIRC/225/Rev.4 (Corrected) [4], далее именуемом INFCIRC/225, и составлено оно конкретно для применения в отношении внутренних нарушителей. Его следует

Настоящая публикация была заменена публикацией No. 8-G (Rev. 1).

использовать вместе с документами IAEA-TECDOC-967 (Rev.1) [5] и IAEA-TECDOC-1276 [6].

1.3. ЦЕЛЬ И СФЕРА ПРИМЕНЕНИЯ

Цель настоящего руководства - обеспечить общие руководящие материалы для компетентного органа и операторов[1] по предупреждению и защите от угроз, исходящих от внутренних нарушителей. Угрозы в отношении ядерных установок могут быть связаны с внешними нарушителями, внутренними нарушителями или как с теми, так и с другими, действующими в сговоре.

Термин "угроза" используется для описания вероятной причины причинения вреда людям, нанесения ущерба собственности или вреда окружающей среде лицом или лицами, имеющими мотивацию, намерение и возможность совершить злоумышленное действие. Внутренние нарушители представляют собой серьезную угрозу для установки, поскольку такие нарушители могут использовать имеющиеся у них преимущества обладания санкционированным доступом, полномочиями и знаниями с целью злоупотребления доверием и обхода мер безопасности.

Внутренний нарушитель может занимать на установке любую должность - от сотрудника самого высокого уровня до сотрудника самого низкого уровня. Подробный анализ исходящих от внутреннего нарушителя угроз, естественно, выполняется для установки конкретного типа ввиду существования широкого спектра установок, подлежащих защите (например, исследовательские реакторы, атомные электростанции и другие установки ядерного топливного цикла). Из-за привязки угроз, исходящих от внутреннего нарушителя, к характеру конкретной установки руководящие материалы не включаются в документ общего характера, такой, как INFCIRC/225.

Сфера применения настоящего руководства - в соответствии с документом INFCIRC/225 - охватывает несанкционированное изъятие ядерного материала и саботаж в отношении ядерного материала и ядерных установок. Настоящее руководство применимо к любому типу ядерной установки, в частности, к атомным электростанциям, исследовательским реакторам и другим установкам ядерного топливного цикла (например, заводам по

---

[1] Термин "оператор" используется для описания субъекта (лица или организации), уполномоченного эксплуатировать ядерную или радиационную установку или уполномоченного использовать, хранить или перевозить ядерный материал и/или радиоактивный материал. Как правило, такой субъект будет иметь лицензию или другой разрешающий документ, выданный компетентным органом, или будет являться подрядчиком владельца такого разрешения.

Настоящая публикация была заменена публикацией No. 8-G (Rev. 1).

обогащению, заводам по переработке, заводам по изготовлению топлива и хранилищам), находящимся в эксплуатации, состоянии останова или в процессе снятия с эксплуатации.

Настоящее руководство следует применять на стадиях проектирования, строительства, ввода в эксплуатацию и эксплуатации новых установок. Руководство охватывает также несанкционированное изъятие ядерного материала и саботаж при перевозке ядерного материала. Представленные в настоящем руководстве руководящие материалы и меры можно также применять к физической защите других материалов, включая радиоактивные источники или радиоактивные отходы.

Используемая в настоящем руководстве терминология соответствует определениям, которые приводятся в КФЗЯМ и Поправке к ней 2005 года [1, 2] и/или в Глоссарии "Гарантии МАГАТЭ" [7].

2. ОПРЕДЕЛЕНИЕ УГРОЗ, ИСХОДЯЩИХ ОТ ПОТЕНЦИАЛЬНЫХ ВНУТРЕННИХ НАРУШИТЕЛЕЙ

В данном разделе приводятся руководящие материалы для определения угроз, исходящих от потенциальных внутренних нарушителей, на уровне установки. В руководящих материалах в качестве отправной точки используется информация о внутренних нарушителях, приведенная в проектной угрозе или в других документах государственного уровня, таких, как оценка национальной угрозы, и далее в этих материалах на основе тщательного рассмотрения характеристик площадки установки или операции по перевозке определяются признаки внутренних нарушителей.

Проектная угроза - это инструмент, используемый для планирования, проектирования и оценки системы физической защиты. Государству следует учитывать отличительные черты и характеристики потенциальных внутренних нарушителей и должным образом отражать их в проектной угрозе. В разных государствах проектная угроза, в которой отражены внутренние нарушители, может быть подробно составленной или без деталировки.

В случаях, когда проектная угроза для отдельных сфер ядерной деятельности с потенциально ограниченными радиологическими последствиями и последствиями с точки зрения распространения не разработана, меры по защите от внутренних нарушителей следует основывать на мерах, которые предлагаются в разделе 5. Надлежащее осуществление таких

Настоящая публикация была заменена публикацией No. 8-G (Rev. 1).

мер обеспечит соответствующую основу для соблюдения рекомендаций, приведенных в документе INFCIRC/225.

Помимо информации, содержащейся в проектной угрозе, следует оценивать или анализировать и другую информацию по каждой установке или операции по перевозке с целью подготовки описания каждого отдельного сотрудника или типа потенциального внутреннего нарушителя, исходя из уровня доступа, полномочий по отношению к другим сотрудникам и их знаний в области эксплуатации установки, осуществления перевозок и других общих потенциальных возможностей, способствующих совершению или попытке совершения злоумышленных действий.

Внутренние нарушители могут иметь разную мотивацию и могут быть пассивными или активными, не прибегающими или прибегающими к насилию (рис. 1). Термин "мотивация" используется для описания движущихся сил, побуждающих нарушителя совершить или попытаться совершить злоумышленное действие. Мотивация может включать идеологические, личные, финансовые и психологические факторы, а также другие побудительные факторы, такие, как принуждение. Внутренние нарушители могут действовать независимо или в сговоре с другими лицами. В зависимости от мотивации их действия могут стать злоумышленными спонтанно или быть преднамеренными и хорошо подготовленными.

То или иное лицо может быть принужденным стать внутренним нарушителем в результате принуждения его самого или членов его семьи.

Пассивные внутренние нарушители не прибегают к насилию и ограничивают свое участие предоставлением информации, которая может помочь нарушителям совершить или попытаться совершить злоумышленное действие.

Активные внутренние нарушители проявляют готовность предоставлять информацию, совершать действия и могут быть как прибегающими, так и не прибегающими к насилию. Активные внутренние нарушители готовы открывать двери или замки, оказывать практическую помощь и содействовать в нейтрализации персонала сил реагирования. Не прибегающие к насилию

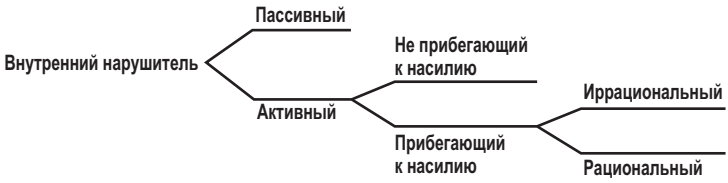

Рис. 1. Категории внутренних нарушителей

Настоящая публикация была заменена публикацией No. 8-G (Rev. 1).

активные внутренние нарушители не желают быть опознанными или идти на риск вступления в столкновения с силами реагирования и могут ограничивать свои действия вторжением в системы учета и контроля, а также системы безопасности и физической (охранной) безопасности. Прибегающие к насилию активные внутренние нарушители могут использовать силу вне зависимости от того, увеличивает ли это их шансы на успех или нет; они могут действовать как рационально, так и иррационально.

Как минимум, следует учитывать указанное ниже.

a) Внутренние нарушители могут занимать в организации любую должность (например, экспериментатора, проектировщика систем физической защиты, сотрудника службы безопасности, сотрудника, работающего с материалом, клерка, сотрудника, ответственного за хранение, сотрудника по гарантиям, сотрудника из числа эксплуатационного персонала и персонала технического обслуживания или руководителя старшего звена). Следует рассматривать также служащих, не являющихся штатными сотрудниками оператора, но обладающих доступом (таких, как поставщики, персонал аварийных служб, включая пожарных и лиц, принимающих первые ответные меры, подрядчиков, субподрядчиков и инспекторов регулирующих организаций).

b) Внутренние нарушители могут обладать:
   i) доступом к некоторым или ко всем участкам установки, системам, оборудованию или инструментам;
   ii) полномочиями в отношении руководства операциями или персоналом;
   iii) знаниями о плане расположения установки, о мерах по организации перевозки и/или процессах перевозки, физической защите, системах безопасности и о другой чувствительной информации;
   iv) техническими навыками и опытом;
   v) разрешением на получение и использование инструментов, оборудования, оружия или взрывчатых веществ.

Поэтому внутренние нарушители могут иметь возможность для совершения злоумышленного действия в случае нормального режима эксплуатации установки, при проведении работ по техническому обслуживанию при перевозке ядерного материала или в аварийных ситуациях, и могут выбирать для этого наиболее благоприятное время.

Помимо потенциальных внутренних нарушителей, определяемых по имеющейся у них возможности получать санкционированный доступ, следует уделять особое внимание людям, не имеющим доступа к установке или операциям по перевозке, но обладающим достаточными знаниями и/или

Настоящая публикация была заменена публикацией No. 8-G (Rev. 1).

полномочиями для совершения злоумышленного действия (например, руководящим сотрудникам центрального аппарата, выписывающим поддельный заказ на доставку во внешнее предприятие). В качестве альтернативы эти сценарии могут быть охвачены оценкой уязвимости, проводимой в отношении внешних нарушителей.

3. СИТУАЦИИ, КОТОРЫЕ СЛЕДУЕТ УЧИТЫВАТЬ ПРИ АНАЛИЗЕ УГРОЗ, ИСХОДЯЩИХ ОТ ВНУТРЕННИХ НАРУШИТЕЛЕЙ

Определенные ситуации на ядерных объектах могут быть благоприятствующими или способствующими реализации угроз, исходящих от внутренних нарушителей.

Ситуации, возникающие на установке или при транспортировке, в том числе ситуации, связанные с вопросами, касающимися персонала, трудовой занятости, такими, как служебные аттестации, политика в области отношений с промышленностью и отсутствие программ формирования культуры физической безопасности, повышения информированности о физической безопасности и установления благонадежности, могут благоприятствовать или способствовать попыткам внутренних нарушителей совершить злоумышленные действия.

Временные ситуации, которые возникают, например, в случае проведения работ по техническому обслуживанию, могут приводить к значительному увеличению числа разрешений на доступ, выдаваемых, например, компаниям-подрядчикам.

Благоприятствовать угрозам, исходящим от внутренних нарушителей, могут и ситуации, возникающие за пределами установки или поблизости от маршрутов перевозки, в том числе в связи с общим отношением общественности как в городской, так и в сельской прилегающей местности, а также присутствием организованных враждебных групп. Следует принимать во внимание наличие любых недовольных групп населения и враждебного социально-политического настроя. Особое внимание следует уделять возможным связям между этими группами и лицами, обладающими опытом эксплуатации установки или имеющими доступ к ядерной установке.

При рассмотрении угроз, исходящих от внутренних нарушителей, оператору следует учитывать такие ситуации.

Настоящая публикация была заменена публикацией No. 8-G (Rev. 1).

4. ОПРЕДЕЛЕНИЕ ЦЕЛЕЙ

Задача данного раздела - обеспечить общие руководящие материалы для определения потенциальных целей применительно к несанкционированному изъятию ядерного материала и актам саботажа, уделяя при этом особое внимание целям, привлекательным для внутренних нарушителей. В других публикациях МАГАТЭ, таких, как [4], приводятся более подробные руководящие материалы по определению целей.

4.1. ОБЩИЙ ОБЗОР

Определение целей – это оценка того, что необходимо защищать изначально, включая ядерный материал, связанные с ним участки, здания и оборудование, элементы, системы и функции, - без учета трудности обеспечения защиты.

Следует учитывать:

a) анализ безопасности и связанный с ним анализ определения особо важных зон, см. [4], пункт 7.1.5, в качестве отправной точки для определения потенциальных целей саботажа;
b) классификацию ядерного материала по категориям в ее применении к физической защите ядерного материала (INFCIRC/225) для определения потенциальных целей, которые могут стать предметом несанкционированного изъятия [4];
c) проектную угрозу или другие документы государственного уровня, такие, как оценка национальной угрозы, в которых приводится информация или критерии для определения потенциальных целей.

Цели внутренних нарушителей несколько отличаются от целей внешних нарушителей. Так, например, внутренние нарушители могут на протяжении длительного времени совершать хищения небольших количеств ядерного материала из нескольких мест, и ни в одном из этих мест количество материала не будет привлекательным для внешнего нарушителя. Кроме того, в ряде случаев последовательность злоумышленных действий внутреннего нарушителя, ведущая к саботажу, может быть не ограниченной по времени, тогда как действия внешнего нарушителя находятся в зависимости от времени.

Следует проводить анализ с целью ранжирования целей, которые были определены, по серьезности последствий. Это ранжирование обеспечит основу для принятия многоуровневых предупредительных и защитных мер.

Настоящая публикация была заменена публикацией No. 8-G (Rev. 1).

4.2. ЦЕЛИ САБОТАЖА

Уровни неприемлемых радиологических последствий устанавливаются государством или компетентным органом и в различных государствах могут быть разными. Желательно, чтобы при уточнении уровней радиологических последствий, используемых применительно к инцидентам, являющимся результатом злоумышленных действий, учитывались критерии безопасности. Однако уровни неприемлемых радиологических последствий в отношении злоумышленных действий могут отличаться от уровней, которые учитывались при анализе безопасности установки, и может потребоваться их классификация по уровням ниже или выше тех, которые применялись для анализа безопасности.

Определение целей саботажа на установке начинается с использования документации по техническому обоснованию безопасности, включая вероятностный анализ безопасности в отношении внешних событий, если таковой существует, и других источников, могущих помочь в определении возможных аварийных последовательностей, которые могут иметь значительные радиологические последствия для работников, населения и окружающей среды. Аварийная последовательность - это череда событий, являющихся результатом одного или нескольких исходных событий (ошибка человека, отказ одного или нескольких элементов или одной или нескольких функций), которые приводят к тому, что установка находится в поврежденном состоянии несмотря на установленные на ней инженерно-технические системы безопасности и устройства для смягчения последствий.

Саботаж, однако, не учитывается в вероятностном анализе безопасности, и поэтому его необходимо принимать во внимание, поскольку другие события, которые могут быть инициированы злоумышленным действием, также могут приводить к значительным радиологическим последствиям. Например, в некоторых случаях одновременный отказ резервного оборудования системы, связанной с безопасностью, не рассматривается как вероятный в вероятностном анализе безопасности. Однако такой отказ может реально произойти в результате акта саботажа и способен вызвать радиологические последствия. Следует определить те элементы, системы или функции, выход из строя или отказ которых в результате злоумышленного действия мог бы иметь серьезные последствия.

Этот подход позволяет выявлять наиболее чувствительные элементы на установке (компоненты, системы или функции) и определять место их расположения.

Настоящая публикация была заменена публикацией No. 8-G (Rev. 1).

4.3. ЦЕЛИ, КОТОРЫЕ МОГУТ СТАТЬ ПРЕДМЕТОМ НЕСАНКЦИОНИРОВАННОГО ИЗЪЯТИЯ

При определении потенциальных целей для несанкционированного изъятия ядерного материала следует учитывать как

a) неоднократное несанкционированное изъятие небольших количеств ядерного материала в течение нескольких эпизодов (хищения на протяжении длительного времени), так и
b) несанкционированное изъятие большого количества ядерного материала в течение одного эпизода (внезапное хищение).

Чтобы охватить эти оба варианта, следует учитывать инвентарное количество всего ядерного материала на установке или в процессе перевозки. Следует обеспечить, чтобы список инвентарного количества включал объем, форму, место нахождения и состояние всего ядерного материала на установке или в процессе перевозки.

Цели хищения следует определять на основе информации или критериев, содержащихся в документе государственного уровня. В качестве альтернативы цели могут быть отнесены к группам в одной из трех категорий (I, II и III) в соответствии с таблицей классификации ядерного материала, приводимой как в КФЗЯМ [1], так и в INFCIRC/225 [4]. Это распределение по группам следует основывать на оценке риска использования материала в целях создания ядерного взрывного устройства, что само по себе зависит от: типа материала, например плутоний, уран; изотопного состава, т.е. содержания делящихся изотопов; физической и химической формы; степени разбавления; уровня излучения; и количества. Кроме того, при определении целей, которые могут стать объектом несанкционированного изъятия ядерного материала внутренними нарушителями, следует учитывать возможность того, что нарушитель соберет из нескольких мест нахождения, относящихся к более низкой категории классификации, количество материала, эквивалентное более высокой категории классификации.

Настоящая публикация была заменена публикацией No. 8-G (Rev. 1).

5. МЕРЫ В ОТНОШЕНИИ ВОЗМОЖНЫХ ВНУТРЕННИХ НАРУШИТЕЛЕЙ

В данном разделе приводится описание подхода к противодействию угрозе, исходящей от внутреннего нарушителя, и даются рекомендации по конкретным предупредительным мерам и защитным мерам.

5.1. ОБЩИЙ ПОДХОД

Термин "предупредительные меры" используется для описания мер, направленных на то, чтобы воспрепятствовать угрозам, исходящим от возможных внутренних нарушителей, или устранить их, либо на то, чтобы свести к минимуму возможности для создания угроз или предотвратить осуществление злоумышленного действия. Термин "защитные меры" используется для описания мер, направленных на выявление, задержку осуществления злоумышленных действий и реагирование на осуществляемые злоумышленные действия, а также на смягчение или сведению к минимуму их последствий. В соответствии с установленным порядком защитные меры следует координировать с общими планами аварийного реагирования. В планы аварийного реагирования следует также на случай несанкционированного изъятия ядерного материала включать положения по его возвращению. Следует предусматривать, чтобы предупредительные и защитные меры обеспечивали глубокоэшелонированную защиту и были полностью интегрированы в хорошо разработанную программу по физической безопасности. Подход, который следует использовать для предупреждения злоумышленных действий внутренних нарушителей и защиты от них, представлен на рис. 2.

Рис. 2. Подход к предупреждению злоумышленных действий внутренних нарушителей и защите от них.

Настоящая публикация была заменена публикацией No. 8-G (Rev. 1).

На рис. 2 стрелками между прямоугольниками показаны последовательные шаги, образующие подход к предупреждению и защите применительно к возможным внутренним нарушителям, характеристики которых даны в разделе 2.

Цели предупреждения:

1) исключение появления возможных внутренних нарушителей путем выявления подозрительного поведения или признаков, которые могут указывать на мотивацию до получения ими разрешения на доступ;
2) исключение появления дополнительных возможных внутренних нарушителей путем выявления подозрительного поведения или признаков, которые могут указывать на мотивацию после получения ими доступа;
3) сведение к минимуму возможностей совершения злоумышленных действий путем ограничения доступа, полномочий и знаний, а также путем принятия других мер.

Цели защиты:

4) выявление, задержка злоумышленных действий и реагирование на них;
5) смягчение или сведение к минимуму последствий.

Многие меры, перечисленные в разделах 5.3 и 5.4, можно считать как предупредительными, так и защитными мерами. Предложенный перечень следует рассматривать лишь как один из возможных вариантов. Рекомендуется, чтобы каждая из предлагаемых мер рассматривалась и применялась с учетом ее индивидуальных особенностей применительно к целям предупреждения или защиты.

5.2. РАЗРАБОТКА ВСЕОБЪЕМЛЮЩЕГО ПОДХОДА

Общий подход заключается в создании нескольких эшелонов (рубежей) защиты, включающих как административные средства (процедуры, инструкции, административные санкции, правила контроля доступа, правила соблюдения конфиденциальности), так и технические средства (несколько эшелонов защиты с оборудованием для обнаружения и задержки), которые внутренним нарушителям придется преодолевать или обходить для достижения своих целей.

Настоящая публикация была заменена публикацией No. 8-G (Rev. 1).

Из-за доступа, знаний, полномочий и характеристик, которыми обладают внутренние нарушители (как это определено в разделе 2), применение предупредительных и защитных мер в целях противодействия угрозам, исходящим от внутренних нарушителей, обычно является гораздо более трудным делом, чем осуществление мер по противодействию угрозам, исходящим от внешних нарушителей. Поэтому, несмотря на то, что решение ряда вопросов уже предусматривается применительно к угрозам, исходящим от внешних нарушителей, следует принимать во внимание любые элементы, которые могут обеспечить защиту от угроз, исходящих от внутренних нарушителей. Эти элементы включают те возможности по выявлению, задержке, реагированию и смягчению последствий, которые обеспечивают положения по безопасности, радиационной защите и КиУМ. Следует определять их синергетический эффект и интегрировать их во всеобъемлющий подход.

Для целей ядерной безопасности соблюдение проектных критериев, таких, как резервирование или неодинаковость в системах и оборудовании, важных для безопасности, или критериев компоновки, таких, как физическое или географическое разделение или изоляция друг от друга этих систем или оборудования, обеспечивается на этапе проектирования установки или транспортной упаковки. Благодаря этим положениям защита от саботажа может быть улучшена за счет того, что для совершения злоумышленного действия внутреннему нарушителю потребуется больше готовиться, располагать большим набором средств и иметь больше времени. Вследствие этого они могут со значительной эффективностью сдерживать, предупреждать или задерживать акты саботажа со стороны внутренних нарушителей либо смягчать или сводить к минимуму радиологические последствия.

Свой вклад как в сдерживание, так и в предупреждение несанкционированного изъятия или саботажа со стороны внутренних нарушителей могут внести и меры по радиационной защите, такие, как ограничение доступа к конкретным зонам и устройствам для обеспечения радиационной защиты.

Положения по КиУМ предназначены для обеспечения строгого инвентарного учета всего ядерного материала и регистрации тревожного сигнала, если в балансе материала обнаруживается расхождение. КиУМ позволяет также операторам: a) иметь точные данные о всех вводах и выводах ядерного материала на установках по их количеству и типу; b) всегда иметь информацию о месте нахождения, об использовании, о перемещении и превращении ядерного материала; c) обнаруживать любые аномалии в связи с обращением с ядерным материалом. В системе учета ядерного материала следует обеспечивать средства обнаружения несанкционированных передач или неоднократного несанкционированного изъятия небольших количеств

Настоящая публикация была заменена публикацией No. 8-G (Rev. 1).

ядерного материала из установки, которые могут не обнаруживаться с помощью системы физической защиты. Для обнаружения аномалий следует использовать, в частности, печати, устройства, указывающие на вмешательство, и компьютерную систему учета. Необходимо проводить анализ системы КиУМ для определения ограничений и уязвимых мест таких систем.

5.3. ПРЕДУПРЕДИТЕЛЬНЫЕ МЕРЫ

Цель предупредительных мер сводится к исключению появления возможных нарушителей и к минимизации вероятности появления внутренних нарушителей, пытающихся совершить злоумышленные действия. В качестве предупредительных рекомендуются следующие меры:

a) Проверка личности. Проверка личности[2] служит для подтверждения подлинности данного лица. Она подтверждает точность фамилии, имени и персональных данных физического лица.

b) Оценка надежности. Оценка надежности[2] – это начальная и непрерывные оценки добросовестности, честности и надежности лица в ходе проверок до его приема на службу, а также проверок, проводимых в период работы, которые предназначаются для определения мотивации или поведения лиц, которые могут становиться внутренними нарушителями. Эти проверки направлены на определение мотивационных факторов, таких как жадность, финансовые факторы, идеологическая заинтересованность, психологические факторы, желание мести (например, из-за переживаемой несправедливости), физическая зависимость (например, от наркотиков, алкоголя или секса) и факторов, из-за которых лицо может быть подвержено принуждению со стороны внешних нарушителей. Такие факторы могут быть выявлены в результате изучения материалов криминального учета, отзывов с предыдущих мест работы, предыдущего трудового стажа, финансовых документов, медицинской документации и результатов психологических тестов/составления психологического портрета. Периодические проверки следует проводить в период работы, так как некоторые из этих обстоятельств могут быть неочевидными или изменяться со временем. Такое изучение представляет особый интерес в

[2] Национальное законодательство может ограничивать объем или проведение проверки личности и оценок надежности лица в государстве. Положения этого практического руководства применяются без ущерба для законных прав лиц, включая право на надлежащую правовую процедуру, в соответствии с национальным законодательством и/или международным правом.

Настоящая публикация была заменена публикацией No. 8-G (Rev. 1).

случае временных служащих и работников, чьи обязанности могут обусловливать их близкое нахождение по отношению к чувствительным (критическим) целям. Глубину проверок надежности следует дифференцировать в соответствии с уровнем доступа, имеющегося у данного лица (например, в случае доступа к материалам категории III требуется самый низкий уровень проверок надежности и доступа к материалу категории I или особо важным зонам - наивысший уровень проверок надежности). Ее следует определять в соответствии с действиями, описанными в разделах 2-4 настоящего руководства, в которых содержится обоснование для сбора информации.

c) Сопровождение работников и посетителей, нечасто бывающих на объекте, и наблюдение за ними. Временные работники, такие как персонал, выполняющий работы по техническому обслуживанию, ремонту или строительству, часто являются работниками компаний, действующих на основе подряда или субподряда. Надежность временных работников и посетителей не может быть определена до получения ими разрешения на доступ. Сопровождение таких лиц – это способ обеспечить их нахождение в надлежащем месте и выполнение ими должным образом своих обязанностей. Чтобы сопровождение было эффективным, осуществляющим его сотрудникам следует иметь информацию об утвержденных работах, которые будут выполнять эти лица, включая доступ к конкретным местам и действия, которые они будут совершать. Кроме того, патрули охраны могут сдерживать или выявлять любые попытки физических лиц совершать злоумышленные действия.

d) Обеспечение информированности по вопросам физической безопасности. Осуществление хорошей программы информированности персонала и подрядчиков по вопросам физической безопасности способствует поддержанию культуры физической безопасности в организации. Эффективная программа информированности по вопросам физической безопасности включает выработку и применение ясной политики в области обеспечения физической безопасности, применение принудительных мер в отношении практических методов обеспечения физической безопасности и непрерывное обучение. Цель программы обучения сводится к созданию обстановки, в которой все служащие внимательно относятся к вопросам соблюдения политики и процедур в области обеспечения физической безопасности, что позволяет им оказывать содействие в выявлении случаев ненадлежащего поведения или ненадлежащих действий и сообщать об этом. Всем, независимо от выполняемых ими ролей или функций, следует понимать угрозы и потенциальные последствия злоумышленных действий и сознавать свою собственную роль в сокращении рисков и создании всеобъемлющего и

Настоящая публикация была заменена публикацией No. 8-G (Rev. 1).

эффективного режима физической безопасности. В программах информированности по вопросам физической безопасности следует также предусматривать меры, направленные на сокращение рисков шантажа, принуждения, вымогательства или других угроз в отношении служащих и их семей, и следует обеспечивать, чтобы они способствовали тому, чтобы сотрудники сообщали руководителям служб физической (охранной) безопасности о таких актах принуждения или попытках таких действий. Наконец, программы информированности по вопросам физической безопасности следует разрабатывать в координации с программами информированности по вопросам технической безопасности в целях поддержания двух эффективных и дополняющих друг друга культур - безопасности и физической безопасности.

e) Обеспечение конфиденциальности (безопасности информации). Информация о мерах по обеспечению безопасности или чувствительных (критических) целях (например, месте нахождения инвентарного количества ядерного материала, картах площадки или конкретных чертежах оборудования, систем или устройств, которые отражают проектные решения конкретных целей, кодовых комбинациях замков, паролях и конструкции механических ключей) может помочь внутренним нарушителям в успешном совершении злоумышленных действий. Эту информацию следует хранить как конфиденциальную таким образом, чтобы только лица, которым необходимо ее знать, имели разрешение на доступ к ней. Кроме того, следует обеспечивать надежную защиту и разделение информации о потенциальных слабых местах в системах физической защиты, поскольку она может облегчать несанкционированное изъятие ядерного материала или совершение актов саботажа. Разделение означает раздел информации на части, контроль за которыми осуществляется отдельно, с тем чтобы не допустить сбора внутренними нарушителями всей информаций, необходимой для попытки злоумышленного действия. Особое внимание следует уделять электронной информации. Обеспечение конфиденциальности будет означать, что внутренние нарушители должны будут предпринимать дополнительные усилия для осуществления замысла несанкционированного изъятия ядерного материала или совершения акта саботажа, и во время этих усилий в отношении таких нарушителей могут быть задействованы меры по сдерживанию или обнаружению.

f) Обеспечение качества. В целях обеспечения уверенности в том, что требования, определенные для всех видов деятельности, важных с точки зрения предупреждения и защиты от угроз, исходящих от внутреннего нарушителя, соблюдаются, следует установить и осуществлять политику

Настоящая публикация была заменена публикацией No. 8-G (Rev. 1).

и программы обеспечения качества. Это относится не только к предупреждению, но также и к другим первичным функциям.

g) Удовлетворенность служащих. Нельзя рассчитывать на то, что только потому, что данное лицо является служащим или подрядчиком, он или она не будет испытывать чувства неудовлетворенности. Поэтому установлению хороших взаимоотношений между работниками и между руководством и работниками следует уделять должное внимание, и следует обеспечивать, чтобы эти взаимоотношения были частью культуры физической безопасности. Руководителям следует обеспечивать подготовку, позволяющую им выявлять случаи несоответствующего поведения служащего во взаимоотношениях с определенными лицами, например старшим руководителем, руководителем службы физической безопасности или консультантом по кадрам, и заострять на этом внимание. Осуществление политики карьерного роста, которая преследует цель подготовки всех служащих для перехода на следующую более высокую должность в организации, поможет создать резерв подготовленных специалистов, могущих заменить сотрудника, занимающего данную должность, который выбывает из штата организации даже в ближайшее время, а также будет способствовать обеспечению качества.

h) Физическое разделение зон. Разделение доступа к установкам посредством мер контроля доступа сводит к минимуму возможность саботажа или несанкционированного изъятия ядерного материала внутренними нарушителями, затрудняя получение данных, относящихся к физической безопасности, целям, и ограничивая способность совершать злоумышленные действия. Следует принимать все возможные меры для обеспечения того, чтобы один человек не получал все необходимые официальные разрешения на доступ, которые позволили бы такому лицу совершить злоумышленное действие. Степень физического разделения зон необходимо устанавливать соответственно потенциальным рискам; поэтому большинство чувствительных целей следует размещать в хорошо защищенных (охранных) зонах, в то время как менее чувствительные цели могут располагаться в менее защищенных зонах. В разделенных зонах следует применять правила необходимости доступа, аналогичные правилам необходимости знать, которые применяются к чувствительным (критическим) документам и информации. Введение строгих ограничений в отношении числа лиц, имеющих доступ в чувствительную зону, а также числа лиц, уполномоченных выдавать официальные разрешения на доступ в чувствительные зоны, может свести к минимуму возможности, которыми располагают внутренние нарушители. На стадии

Настоящая публикация была заменена публикацией No. 8-G (Rev. 1).

проектирования особое внимание следует уделять сведению к минимуму излишнего доступа в защищенные зоны.

i) Разделение видов работы. Разделение видов работы будет ограничивать способность внутренних нарушителей иметь необходимые потенциальные возможности для совершения злоумышленного действия. Такие потенциальные возможности могут включать возможность использования специальных инструментов и оборудования, требующихся для выполнения определенных операций или для обращения с материалом. Перемещение инструментов, материалов и оборудования из одной зоны в другую следует осуществлять с соблюдением формальных процедур, и с целью сведения к минимуму возможности несанкционированного изъятия ядерного материала внутренними нарушителями следует предусматривать участие в этих процедурах более чем одного человека.

j) Санкции (дисциплинарные меры и судебное преследование). Важно, чтобы потенциальные внутренние нарушители знали, что в случае преднамеренного нарушения законов и регулирующих правил или инструкций оператора могут быть применены строгие санкции. Неизбежность дисциплинарных мер и судебного преследования может сдерживать внутренних нарушителей от совершения злоумышленных действий. Кроме того, требование, чтобы операторы информировали компетентные органы о каждом злоумышленном действии или попытке его совершить, будет обеспечивать после проведения соответствующего анализа обмен информацией в рамках обратной связи с другими операторами и при необходимости возможное обновление регулирующих требований.

5.4. ЗАЩИТНЫЕ МЕРЫ

Цель защитных мер сводится к выявлению, задержке осуществления злоумышленных действий и реагированию на эти действия после их начала, а также к смягчению или сведению к минимуму последствий. При разработке и осуществлении защитных мер следует предпринимать усилия для обеспечения того, чтобы эти меры оказывали минимальное воздействие на радиационную защиту, безопасность или системы аварийного реагирования. В случае коллизии требований необходимо принимать решение, которое сводит к минимуму совокупный риск для персонала и населения. В качестве защитных мер рекомендуется следующее.

Настоящая публикация была заменена публикацией No. 8-G (Rev. 1).

5.4.1. Выявление

Злоумышленные действия могут быть выявлены посредством применения защитных датчиков, наблюдения за персоналом и/или мониторинга рабочих процессов. В случае внешних нарушителей меры по выявлению сосредоточиваются на обнаружении проникновения нарушителями через эшелоны (рубежи) защиты. Выявление злоумышленных действий, совершаемых внутренними нарушителями, - это более трудный процесс. Внутренние нарушители способны обходить многие меры по выявлению благодаря имеющемуся у них доступу или другим доступным им средствам. Поэтому меры защиты от угроз, исходящих от внутренних нарушителей, следует сосредоточивать на выявлении внутренних нарушителей как во время самих актов, так и во время подготовительных (несанкционированных) действий, таких как манипуляция оборудованием, обеспечивающим безопасность, или фальсификация записей КиУМ. Следовательно, выявление внутренних нарушителей может происходить гораздо позднее в последовательности событий при развитии инцидента, чем выявление внешних нарушителей.

Для того чтобы выявление было эффективным, необходимо проводить его оценку. Надлежащее и оперативное проведение оценки характера акта, совершенного внутренним нарушителем, может оказаться сложным делом. Эта сложность может серьезно ослаблять способность своевременного реагирования.

Поскольку выявление злоумышленных действий, совершаемых внутренними нарушителями, сильно зависит от мер по наблюдению и контролю, обеспечение более длительной задержки действий внутреннего нарушителя может повышать вероятность выявления; следовательно, увеличение числа физических барьеров или повышение сложности исполнения злоумышленного действия может обеспечить дополнительные возможности для выявления или даже сдерживания внутренних нарушителей от попытки совершения злоумышленного действия.

Цели наблюдения состоят в обеспечении уверенности в том, что деятельность любого уполномоченного сотрудника всегда контролируется по меньшей мере еще одним опытным, уполномоченным сотрудником, с тем чтобы несанкционированные действия одного из них могли быть немедленно обнаружены и доведены до сведения тех, кого это касается (применяется «правило двух лиц»). Этот метод обнаружения способен обеспечить механизм оперативной выработки и оценки тревожного сигнала. Наблюдение может осуществляться с привлечением для этой цели коллег, руководителей или с помощью кабельного телевидения. В случае совершения злоумышленного действия видеоматериалы могут использоваться для определения круга

Настоящая публикация была заменена публикацией No. 8-G (Rev. 1).

возможных подозреваемых. В действительности без мониторинга своевременная оценка злоумышленных действий может быть затруднена. Метод, который может использоваться для выявления внутренних нарушителей, - это наблюдение во время работы, проводимое с целью проверки возможного осуществления несанкционированных действий. Этот метод будет полезен в случаях, когда работа по обслуживанию оборудования выполняется не полностью или когда для выполнения определенной операции отбирается одно количество ядерного материала, а в учетных документах регистрируется другое количество.

Правило двух лиц требует, чтобы по меньшей мере два опытных работника контролировали друг друга в чувствительной зоне. Требования этой базовой процедуры предусматривают, чтобы по меньшей мере два человека находились в чувствительной зоне таким образом, чтобы каждый из них мог контролировать выполнение всех действий в соответствии с предписаниями. Следует обеспечивать, чтобы каждый из двух человек, которые участвуют в выполнении рабочего задания, имели соответствующую техническую квалификацию, которая позволяет им немедленно обнаруживать несанкционированные действия. Кроме того, следует предусматривать механизм немедленного сообщения о подозрениях в злоумышленных действиях или подозрительной деятельности. Если последующие расследования показывают, что никаких злоумышленных действий не было, важно, чтобы ни к какой из сторон не применялись санкции в связи с ложной тревогой, так как в противном случае партнеры будут впоследствии отказываться сообщать о подозрительном поведении. На это следует обращать внимание в процессе обучения по программе информированности по вопросам физической безопасности. Чтобы два человека действовали эффективно, они должны оставаться постоянно и полностью в поле зрения друг друга и должны быть в полной мере информированы о санкционированных работах, которые выполняет каждый из них. В идеальном случае правило двух лиц предусматривает поручение двум компетентным работникам выполнение работы одного человека. Правило двух лиц работает эффективно до тех пор, пока у соответствующих лиц не появляется состояние благодушия в результате развития дружеских отношений или общения в течение длительного времени. Когда это возможно, руководителям следует обеспечивать, чтобы осуществлялась ротация членов таких групп, состоящих из двух человек. Применение правила двух лиц при предоставлении доступа в чувствительные зоны является средством сдерживания и может помочь работе по выявлению. Кроме того, правило двух лиц может помочь в обеспечении защиты от вмешательства в систему датчиков, осуществляемого внутренними нарушителями.

Настоящая публикация была заменена публикацией No. 8-G (Rev. 1).

Контроль доступа используется для обеспечения исключительно санкционированного входа или выхода, а также для предупреждения или обнаружения несанкционированного проникновения и выхода. Контроль доступа достигается путем удостоверения личности физических лиц посредством идентификационного устройства (одной или нескольких карточек или ключей), кода доступа (кодовой комбинации замка или персонального идентификационного номера) и/или личного идентификатора (биометрии). Следует обеспечивать, чтобы контроль доступа также охватывал транспортные средства. Кроме того, контроль доступа может использоваться для установления присутствия людей в разных зонах. Соответствующим образом зарегистрированные записи в системе контроля доступа могут использоваться при проведении расследования в отношении злоумышленного действия для определения круга возможных подозреваемых. Перед выдачей официального разрешения на доступ в чувствительную зону следует устанавливать конкретные критерии (такие как необходимость выполнения данной операции, необходимость сопровождения, необходимость знать и надежность). Лица, которым предоставляется доступ в чувствительную зону, должны соответствовать этим критериям. Оборудование, используемое для изготовления карточек, и системы предоставления доступа следует защищать в целях предотвращения несанкционированного предоставления доступа. Кроме того, систему предоставления доступа следует периодически проверять для обеспечения того, чтобы она функционировала эффективно.

Отслеживание перемещения и мест нахождения персонала на объекте способствует обеспечению защиты от нарушения правил доступа, а также позволяет получить полезную информацию после инцидента. Имеющиеся в настоящее время технологии обеспечивают возможность отслеживать нахождение каждого работника на всей территории объекта благодаря регистрации мест нахождения и зон, в которых ежедневно бывает работник, и фиксации времени, в течение которого он находится в каждом месте. Информация о том, что на объекте имеется система слежения, может сдерживать работника от совершения несанкционированных действий. Более того, данные системы отслеживания могут использоваться при проведении расследования злоумышленного действия для составления начального списка подозреваемых.

Для совершения злоумышленного действия внутренним нарушителям могут требоваться инструменты, материалы и орудия, которые не доступны или не допускаются для доставки на объект. Поэтому следует проводить проверки с целью предотвращения и обнаружения доставки запрещенных предметов в чувствительные зоны. В число запрещенных предметов могут входить неразрешенные инструменты и материалы, материалы защиты от излучений, оружие и взрывчатые вещества, так как они могут использоваться для

Настоящая публикация была заменена публикацией No. 8-G (Rev. 1).

получения доступа к чувствительным (критическим) элементам или причинения им ущерба, а также для хищения ядерного материала. Следует обеспечивать, чтобы строгость досмотров соответствовала чувствительности зоны, и досмотры вблизи от цели следует также проводить с еще большей строгостью.

Методы обнаружения запрещенных предметов включают ручной досмотр персонала, упакованных грузов и транспортных средств; использование металлодетекторов, рентгеновских установок и детекторов излучения; и использование служебных собак и детекторов взрывчатых веществ. При использовании этих методов следует учитывать специфические особенности объекта и угрозы, от которых требуется защита. При определении мест, в которых должны проводиться досмотры, следует обеспечивать, чтобы они не располагались на значительном удалении от чувствительных зон так, чтобы можно было легко обходить проверки. Например, внутренние нарушители могут действовать в обход проверок на границе защищенной зоны, перебросив запрещенные предметы через ограждение защищенной зоны и позднее изъяв их оттуда. Поскольку досмотр транспортных средств является более трудным делом, чем досмотр персонала, целесообразно в значительной мере ограничивать число транспортных средств, которым разрешается въезд в чувствительные зоны.

В случае определенных типов ядерного материала следует использовать детекторы излучения для обнаружения несанкционированного изъятия материала при его выносе лицами, вывозе в упаковках или транспортных средствах из защищенной зоны. Детекторы излучения могут размещаться в проходах вместе с металлодетекторами для повышения эффективности проверки, так как для изъятия ядерного материала из ядерной установки может использоваться экранирующий материал. Для контроля лиц и материала на выходе из зоны может также применяться ручной досмотр. Применение досмотра на основе случайной выборки может сдерживать несанкционированное изъятие ядерного материала. Если это не противоречит правилам безопасности, следует предусматривать блокировку выхода при срабатывании сигнализации системы безопасности. Особое внимание следует уделять условиям проведения аварийной эвакуации, включая учения, с точки зрения предупреждения несанкционированного изъятия ядерного материала. Во время детального осмотра грузового транспортного средства перед его загрузкой и отправкой особое внимание следует уделять обеспечению того, чтобы лица, проводящие осмотр, не могли оставить предметы, которые могли бы способствовать совершению злоумышленного действия.

Мониторинг нормального осуществления процессов или деятельности может использоваться в целях наблюдения за данной зоной, выявления несанкционированных действий или обеспечения ранней оценки тревожных

Настоящая публикация была заменена публикацией No. 8-G (Rev. 1).

сигналов. Проверка эксплуатационных параметров ядерной установки (значений температуры, давления, расхода, сигналов радиационного мониторинга и т.д.) осуществляется непрерывно для обеспечения того, чтобы эти параметры оставались в рамках эксплуатационных пределов. Следует обеспечивать, чтобы тревожная сигнализация срабатывала в случае, когда один из этих параметров превышает предписанное пороговое значение. Так как саботаж может привести к возникновению ненормальной ситуации, затрагивающей эксплуатационные параметры, осуществление контроля за эксплуатационными параметрами может способствовать выявлению злоумышленных действий.

Чрезвычайно важно установить процедуру передачи сигналов тревоги между эксплуатационным персоналом и персоналом службы безопасности для обеспечения того, чтобы сигналы тревоги быстро передавались персоналу службы безопасности на центральном пульте охраны. Следует обеспечивать, чтобы сообщение о срабатывании тревожной сигнализации передавалось еще до того, как эксплуатационный персонал проведет оценку вызвавшей его причины (злоумышленный акт или случайное событие).

Эксплуатационному персоналу следует осуществлять контроль за чувствительным оборудованием, чувствительными системами или устройствами с целью обеспечения уверенности в отсутствии нарушения функций или постороннего вмешательства или с целью обеспечения своевременного обнаружения такого нарушения функций или постороннего вмешательства.

Выполнение регламентных работ, предусматривающих проведение испытаний и технического обслуживания, в значительной мере влияет на эксплуатационную готовность оборудования, а также на возможности предупреждения или устранения неисправностей или отказов, которые могут возникать в результате злоумышленных действий. Эти работы могут быть очень эффективными с точки зрения выявления возможных злоумышленных действий, совершаемых в отношении оборудования или систем, в связи с защитой ядерного материала или чувствительных зон. Если регламентные работы, предусматривающие проведение испытаний или технического обслуживания, приводят к изменению начальных параметров системы, следует выполнять перекалибровку этой системы. Перекалибровку рекомендуется проводить независимо от того, какие работы (испытания или техническое обслуживание) привели к такому изменению. Данный подход способствует обеспечению как предупреждения путем сдерживания (из-за боязни последствий), так и выявления злоумышленных действий.

Одной из мер по смягчению последствий злоумышленного действия является обеспечение быстрой замены частей, которые были повреждены. Для успешного достижения желаемой цели целесообразно обеспечивать защиту

Настоящая публикация была заменена публикацией No. 8-G (Rev. 1).

запасных частей так, чтобы трудно было разрушить или испортить как установленные части, так и запасные части особо важного оборудования. Такую защиту можно обеспечить, например, посредством установки барьеров, хранения запасных частей на удалении от смонтированной части и частого контроля мест хранения.

Инспекции и проверки, в частности необъявленные инспекции и проверки, могут быть эффективным средством предотвращения и защиты от несанкционированного изъятия ядерного материала и саботажа. Инспекции и проверки позволяют обнаруживать испорченное оборудование или ненормальные условия и, таким образом, могут обеспечивать уверенность операторов, компетентного органа или государства в том, что предупредительные и защитные меры эффективно осуществляются.

5.4.2. Задержка действий

Задержку в осуществлении замысла обеспечивают персонал, процедуры или физические барьеры, которые увеличивают время, требующееся для совершения действий нарушителем. Большинство барьеров проектируется так, чтобы они обеспечивали задержку проникновения в помещения или зоны, а не задержку совершения злоумышленных действий и, таким образом, обеспечивают лишь ограниченное противодействие внутренним нарушителям. Однако можно создавать барьеры, которые будут обеспечивать задержку злоумышленных действий вблизи от оборудования или материалов. Например, запирание с помощью замков такого оборудования, как клапаны или распределительный щит, создает задержку для внутренних нарушителей, пытающихся совершить акт саботажа. Барьеры, располагающиеся вблизи от оборудования или материала, особенно эффективны, если данная зона находится под непрерывным наблюдением.

В случае внутренних нарушителей, не имеющих доступа к определенным зонам или материалу, установка барьеров, которые нарушитель не может преодолеть без использования запрещенных предметов и узкоспециализированной подготовки, еще более укрепляет меры по предупреждению за счет фактора сдерживания и повышает вероятность выявления злоумышленных действий. Использование множественных эшелонов различных физических или процедурных барьеров на всех возможных путях проникновения внутренних нарушителей усложняет продвижение внутреннего нарушителя к цели из-за необходимости применения разнообразных инструментов и специальной подготовки. Повышение эффективности барьера, вынуждающее внутренних нарушителей применять более сложные инструменты, приводит к усложнению потребностей в ресурсах, материально-техническом обеспечении, подготовке и специализации. Сложные

Настоящая публикация была заменена публикацией No. 8-G (Rev. 1).

ресурсы могут отсутствовать на объекте, и, вероятно, внутренним нарушителям эти ресурсы необходимо будет доставлять на площадку. Благодаря задержке, достигаемой таким образом в осуществлении злоумышленного действия, обеспечивается возможность выявления и обезвреживания внутренних нарушителей.

Задержки могут также обеспечиваться посредством использования имеющего специальную подготовку персонала службы безопасности, например сотрудников охраны. В некоторых случаях присутствие на местах таких сотрудников может обеспечивать значительную задержку, обусловленную необходимостью обхода этих сотрудников, особенно для внутренних нарушителей, располагающих ограниченными ресурсами.

В результате использования конструкций с учетом требований безопасности систем, которые обеспечивают определенный уровень самозащиты систем, такой как резервирование оборудования, автоматический останов оборудования и автоматическое закрытие клапанов, задача внутреннего нарушителя может усложняться и требовать от него преодоления множественных резервных и рассеянных по объекту установок и оборудования. Такие решения могут обеспечивать задержку в осуществлении злоумышленных действий и препятствовать их успешному совершению.

5.4.3. Реагирование

Реагировать на злоумышленное действие внутреннего нарушителя могут как сотрудники служб безопасности, так и эксплуатационный персонал. Как правило, эксплуатационный персонал реагирует на злоумышленное действие с тем, чтобы изменить его, смягчить или свести к минимуму его последствия, а реагирование персонала служб безопасности направлено на внутренних нарушителей.

В классическом анализе реагирования на угрозы, исходящие от внешнего нарушителя, производится сравнение времени, затрачиваемого силами реагирования, со временем, требующимся для осуществления внешним нарушителем последовательности шагов, необходимых для совершения злоумышленного действия. Косвенным допущением в анализе угрозы, исходящей от внешнего нарушителя, является то, что внешний нарушитель будет легко обнаружен на площадке объекта. Это никак нельзя считать верным применительно к внутренним нарушителям, так как злоумышленное действие, совершенное внутренним нарушителем, может состоять из нескольких актов, отделенных друг от друга во времени и в пространстве. До тех пор, пока внутренние нарушители не определены при выявлении, распознать их среди работников, по-видимому, сложно.

Настоящая публикация была заменена публикацией No. 8-G (Rev. 1).

Как указано выше, внутренний нарушитель не обязательно должен будет выполнять все акты в предписываемом порядке или в быстрой последовательности. Внутренний нарушитель может совершать одиночные акты и затем ждать, чтобы выяснить, обнаружены они или нет. Отсутствие непрерывности в актах, которые внутренние нарушители могут пытаться совершить, может серьезно усложнять процесс реагирования служб безопасности, который необходим для определения и распознавания этих нарушителей. Поэтому расследования будут играть более важную роль в реагировании на угрозы, исходящие от внутреннего нарушителя. Кроме того, может требоваться помощь специалистов по эксплуатации в расследованиях для прогнозирования возможных дальнейших злоумышленных актов, которые могут быть совершены в случае возникновения нештатной ситуации.

Каждому служащему и подрядчику, находящемуся на площадке установки, не только следует быть готовым выявлять злоумышленные действия, но также им следует получить соответствующую подготовку по реагированию с целью защиты себя и установки, и следует знать, что первое действие, которое необходимо предпринять после обнаружения события – это передача тревожного сигнала согласно предписанным процедурам. Процедуры передачи тревожного сигнала следует включать в программу обучения для повышения информированности по вопросам физической безопасности.

Важно понимать, что любые лица, входящие в число тех, кто осуществляет реагирование, могут сами быть внутренними нарушителями, и поэтому процедуры реагирования следует разрабатывать с учетом этого допущения. Например, внутренний нарушитель в группе реагирования может использовать тренировку действий в аварийных условиях, имитировать аварийную ситуацию или создавать фактическую аварийную ситуацию для маскировки злоумышленного действия.

5.4.4. Планы аварийных мероприятий

Планы аварийных мероприятий следует разрабатывать с целью возвращения похищенного ядерного материала и смягчения или сведения к минимуму радиологических последствий саботажа. В планах аварийных мероприятий обычно не проводится различие между внутренними и внешними нарушителями. Следует принимать во внимание тот факт, что внутренние нарушители могут входить в состав группы аварийного реагирования и могут подрывать усилия, направленные на смягчение последствий или возвращение материала.

Подготовку планов аварийных мероприятий, предусматривающих возвращение материала или смягчение последствий, следует осуществлять с целью эффективного противодействия последствиям саботажа или

Настоящая публикация была заменена публикацией No. 8-G (Rev. 1).

несанкционированного изъятия. В эти планы следует включать пункты, касающиеся средств связи, возвращения материала или смягчения последствий, а также оперативные контрмеры, которые должны применяться в случае несанкционированного изъятия ядерного материала или саботажа.

В таких планах должна предусматриваться подготовка сотрудников охраны и сил реагирования по принятию мер в случае злоумышленного действия. Кроме того, следует осуществлять обучение и подготовку другого персонала установки или транспортного подразделения, предусматривающую отработку действий в полной координации с сотрудниками охраны, силами реагирования и группами аварийного реагирования в целях осуществления планов чрезвычайных мер.

В целях исключения возможности изъятия ядерного материала без официального разрешения в планы аварийных мероприятий следует включать процедуры оперативной проверки, позволяющие удостовериться в том, что весь ядерный материал по-прежнему находится на установке или в транспортном средстве. Следует обеспечивать, чтобы процедуры КиУМ позволяли проверять как наличие, так и качество ядерного материала для уверенности в отсутствии замены инертным материалом или имитатором. Эти положения могут дополняться мерами, принимаемыми на уровне государств, в отношении предоставления в случае необходимости информации и технической помощи в целях обнаружения и возвращения утраченного ядерного материала.

В планах аварийных мероприятий следует предусматривать координацию и протоколы для рабочего взаимодействия между операторами и местными, региональными и национальными компетентными органами. Планы аварийных мероприятий на случай инцидентов, являющихся результатом злоумышленных действий, следует разрабатывать и координировать в рамках общих мероприятий по аварийному реагированию. В частности, планы аварийных мероприятий следует разрабатывать и осуществлять в соответствии с международными требованиями по готовности и реагированию в случае ядерной или радиационной аварийной ситуации [8, 9].

6. ОЦЕНКА ПРЕДОХРАНИТЕЛЬНЫХ И ЗАЩИТНЫХ МЕР

6.1. ЦЕЛИ И ОБЩИЙ ОБЗОР ПРОЦЕССА ОЦЕНКИ

Настоящий раздел содержит руководящие материалы по процессу оценки риска, связанного с определенными целями, вызывающими озабоченность.

Настоящая публикация была заменена публикацией No. 8-G (Rev. 1).

Этот процесс оценки является ключевым компонентом оценки риска, предназначенной для выявления мест в системах, уязвимых с точки зрения угроз, исходящих от внутреннего нарушителя. Результат процесса оценки – это оценка эффективности предупредительных и защитных мер в пресечении возможных действий внутреннего нарушителя, которые могут приводить к несанкционированному изъятию ядерного материала или саботажу.

Результаты оценки эффективности мер следует сравнивать с ранее установленными критериями приемлемости. Критерии приемлемости обычно устанавливаются государством или компетентным органом с учетом потенциальных последствий злоумышленных действий и вероятности их успешного осуществления. Если оценка указывает на то, что предупредительные и защитные меры не удовлетворяют необходимым критериям приемлемости, следует вносить в них изменения, направленные на их улучшение.

Кроме того, следует учитывать указанное ниже.

a) Относительную легкость совершения злоумышленного действия. Сценарий, при котором последствия считаются приемлемыми, но который относительно легко осуществить, может быть неприемлемым (например, это может быть несанкционированное изменение порога в параметрах процесса или несанкционированная настройка схемы) и требовать применения корректирующих мер.
b) Уровень риска. Согласно оценке, риск может быть приемлемым, однако при этом он приближается к порогу, при превышении которого уровень риска не является приемлемым. Такой случай не следует исключать из рассмотрения, и рациональная практика управления может требовать принятия дополнительных защитных мер.

Периодически следует проводить повторные оценки эффективности защитных и предупредительных мер, в частности в случаях, когда вносятся изменения в проектные угрозы, в предупредительные и защитные меры или в эксплуатационные условия.

Представленные здесь руководящие материалы применяются в отношении как предупредительных, так и защитных мер, и процесс оценки следует также применять к ним без исключения с целью обеспечения эффективности мер безопасности.

Настоящая публикация была заменена публикацией No. 8-G (Rev. 1).

6.2. ОЦЕНКА ПРЕДУПРЕДИТЕЛЬНЫХ МЕР

Строгая оценка в соответствии с шагами 1 и 2 (исключение появления возможных внутренних нарушителей), описание которой приводится в разделе 5.1, является сложным делом, как и в случае со всеми другими предупредительными мерами, однако считается, что применяемые меры (такие как проверки надежности до приема на службу и в период работы) являются эффективными с точки зрения уменьшения, но не полного исключения возможности появления внутренних нарушителей. Эти меры являются рациональными и целесообразными мерами предосторожности, даже если их действенность не может быть оценена количественно.

Тем не менее эффективное осуществление предупредительных мер поддается проверке, и соответствующие критерии могут быть определены и подвергнуты анализу с целью обеспечения осуществления предупредительных мер в соответствии с проектными решениями. Например, может проводиться анализ числа лиц, которым было отказано в доступе к площадке объекта, лиц, которым закрыт доступ на площадку после увольнения, и инцидентов, о которых поступили сообщения.

Шаг 3 (сведение возможности к минимуму) в подходе к решению задачи предотвращения злоумышленных действий, совершаемых внутренними нарушителями, и защиты от них (описание приводится в разделе 5.1) предусматривает уменьшение возможности получения внутренним нарушителем доступа, полномочий или знаний, необходимых для успешного выполнения злоумышленного действия, приводящего к неприемлемым радиологическим последствиям. Степень и способ ограничения возможности являются важными элементами, которые необходимо учитывать при составлении вероятных сценариев. Поэтому, кроме того, следует проводить систематический анализ, позволяющий определить, какие предупредительные меры, подобные тем, которые предложены в разделе 5.3, предусмотрены и должным образом применяются.

6.3. ОЦЕНКА ЗАЩИТНЫХ МЕР

Меры, используемые для выявления, задержки осуществления злоумышленных действий и реагирования на них, поддаются количественному анализу. Вероятность выявления и своевременность реагирования часто могут быть количественно измерены и, таким образом, обеспечивают основу для анализа эффективности защитных мер.

В представленном процессе признается значение шагов 1, 2 и 3 (см. раздел 5.1) и рекомендуется их рациональное применение, однако основное

Настоящая публикация была заменена публикацией No. 8-G (Rev. 1).

внимание уделяется вопросам оценки эффективности защитных мер, направленных на противодействие злоумышленным действиям. Данный подход включает составление вероятных сценариев действий внутреннего нарушителя, включая при необходимости сценарии сговора с внешними нарушителями, а затем оценку эффективности системы защиты от них.

Составление вероятных сценариев состоит из определения сочетания событий, необходимых для совершения злоумышленного действия. В случае саботажа следует принимать во внимание действия, которые должны быть выполнены для инициирования последовательности, приводящей к неприемлемым радиологическим последствиям. В сценарии саботажа следует включать нападения как на одиночные, так и на множественные цели. В случае несанкционированного изъятия ядерного материала следует определять действия, которые необходимо будет последовательно выполнять для изъятия ядерного материала из установки. В сценарии, охватывающие несанкционированное изъятие ядерного материала, следует включать ситуации, в которых внутренние нарушители покидают объект непосредственно с ядерным материалом или скрывают материал на площадке установки, изымая его позднее при более благоприятных обстоятельствах. Следует учитывать возможность как хищения на протяжении длительного времени, так и внезапного хищения.

При разработке всеобъемлющих сценариев следует рассматривать возможность привязки определенных целей (раздел 4) к определенным группам внутренних нарушителей (раздел 2). Исходя из проектной угрозы, следует определить в конкретном выражении задачи, которые внутреннему нарушителю необходимо будет решить, например ряд действий, которые должны быть осуществлены для достижения цели. В этот ряд действий следует включать рассмотрение как общих действий, так и зон, в которых они осуществляются. Действия могут происходить по определенным путям в пределах установки. Следует определять все элементы защиты, с которыми могут сталкиваться внутренние нарушители на каждом из этих путей или в случае каждого ряда действий. Следует рассматривать все пути, ряды действий по этим путям и защитные элементы, с которыми придется сталкиваться. Так как внутренние нарушители могут осуществлять действия, требующиеся для совершения злоумышленной акции, в течение длительного времени и могут не придерживаться прогнозируемой последовательности, концепция пути не всегда может быть подходящей.

Следует оценивать эффективность элементов защиты применительно к различным стратегиям нанесения ущерба, которые могут использоваться внутренними нарушителями. Стратегии нанесения ущерба строятся путем изучения доступа, полномочий и знаний, которые внутренние нарушители способны использовать для преодоления средств обнаружения и задержки

Настоящая публикация была заменена публикацией No. 8-G (Rev. 1).

осуществления злоумышленных действий. Путем соединения элементов защиты с направленными на нанесение ущерба стратегиями внутреннего нарушителя для данного ряда действий внутреннего нарушителя может быть составлен вероятный сценарий поведения внутреннего нарушителя. Следует отметить, что пути поступления запрещенного материала на установку или несанкционированного изъятия ядерного материала с установки могут не совпадать с путями, используемыми внутренними нарушителями.

После построения детального сценария действий внутреннего нарушителя оценивается эффективность защитных мер путем рассмотрения суммарного эффекта, обеспечиваемого средствами обнаружения, оценки и задержки, а также применения метода наложения мер по реагированию и смягчению последствий на сценарии действий внутреннего нарушителя. Эффективность реагирования будет зависеть как от эффективности пресечения злоумышленного действия, так и от эффективности предупреждения последствий. При проведении оценки следует учитывать возможные попытки внутренних нарушителей снизить эффективность реагирования.

Процесс оценки следует повторять для каждого вероятного сценария. В выводах об эффективности защитных мер следует отражать результаты всех оценок, описанных выше.

После завершения оценки защитных мер полученные результаты можно объединить для завершения расширенного анализа состояния защиты на установке или в транспортном подразделении.

Анализ сценариев позволяет определить возможные усовершенствования защитных мер. Сценарии следует распределять по приоритетности, расположив в виде таблицы данные об эффективности системы защиты для каждой пары цель/внутренний нарушитель, а затем применив заранее определенные критерии для установления приоритета каждого сценария для пары цель/внутренний нарушитель. Используемые для установления приоритета критерии следует основывать на эффективности системы для данного сценария и на потенциальных последствиях его успешного осуществления. Например, для сценариев с низкой эффективностью системы и серьезными вытекающими последствиями следует устанавливать высокий приоритет, в то время как сценариям с высокой эффективностью системы и с малыми последствиями присваивается более низкий приоритет. Первыми следует оценивать сценарии, имеющие наивысший приоритет, для определения возможных усовершенствований системы, которые позволят повысить эффективность системы. Сценарии следует детально изучать на предмет определения возможных усовершенствований. Следует определять действия, в случае которых выявление, оценка и задержка возможны лишь в ограниченной степени или совсем не могут быть реализованы. Сценарии, в которых реагирование может быть замедленным или неэффективным, следует анализировать на

Настоящая публикация была заменена публикацией No. 8-G (Rev. 1).

предмет возможного улучшения реагирования. Возможные решения, принимаемые в указанных ситуациях, могут варьироваться в диапазоне от изменения процедур до применения специального оборудования.

При разработке усовершенствований следует уделять внимание обеспечению того, чтобы усовершенствования защиты применительно к определенным сценариям не приводили к ухудшению работы системы в случае других сценариев, а также не приводили к неприемлемым последствиям для эксплуатационных систем и систем безопасности. Следует вводить в систему предлагаемые усовершенствования и выполнять еще один анализ с целью определения степени достигаемого улучшения. Этот процесс, возможно, необходимо повторять несколько раз, прежде чем будут найдены удовлетворительные, оправданные решения, и ориентированные на достижение определенных показателей обоснования следует документировать с целью подтверждения целесообразности рекомендаций в отношении усовершенствований.

Настоящая публикация была заменена публикацией No. 8-G (Rev. 1).

СПРАВОЧНЫЕ МАТЕРИАЛЫ

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

[2] Физическая ядерная безопасность — меры по защите от ядерного терроризма. Поправка к Конвенции о физической защите ядерного материала. Доклад Генерального директора, GOV/INF/2005/10-GC(49)/INF/6, МАГАТЭ, Вена (2005).

[3] Цели и основополагающие принципы физической защиты, GOV/2001/41, МАГАТЭ, Вена (2001).

[4] Физическая защита ядерного материала и ядерных установок, INFCIRC/225/Rev.4, МАГАТЭ, Вена (1999).

[5] МЕЖДУНАРОДНОЕ АГЕНТСТВО ПО АТОМНОЙ ЭНЕРГИИ, Руководящие материалы и соображения по осуществлению документа INFCIRC/225/Rev.4, IAEA-TECDOC-967(Rev.1)/R, МАГАТЭ, Вена (2002).

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

[7] МЕЖДУНАРОДНОЕ АГЕНТСТВО ПО АТОМНОЙ ЭНЕРГИИ, Гарантии МАГАТЭ. Глоссарий. Издание 2001 года. Серия международного ядерного контроля, № 3, МАГАТЭ, Вена.

[8] МЕЖДУНАРОДНОЕ АГЕНТСТВО ПО АТОМНОЙ ЭНЕРГИИ, Готовность и реагирование в случае ядерной или радиационной аварийной ситуации, Серия норм безопасности МАГАТЭ, № GS-R-2, МАГАТЭ, Вена (2004).

[9] INTERNATIONAL ATOMIC ENERGY AGENCY, Arrangements for Preparedness for a Nuclear or Radiological Emergency, IAEA Safety Standards Series No. GS-G-2.1, IAEA, Vienna (2007).

Настоящая публикация была заменена публикацией No. 8-G (Rev. 1).

Настоящая публикация была заменена публикацией No. 9-C (Rev.1).

IAEA
Международное агентство по атомной энергии

Где заказать публикации МАГАТЭ

В указанных ниже странах публикации МАГАТЭ могут быть приобретены у перечисленных ниже агентов или в крупных местных книжных магазинах. Оплата может производиться в местной валюте или купонами ЮНЕСКО.

Австралия
DA Information Services, 648 Whitehorse Road, Mitcham Victoria 3132
Телефон: +61 3 9210 7777 • Факс: +61 3 9210 7788
Эл. почта: service@dadirect.com.au • Веб-сайт: http://www.dadirect.com.au

Бельгия
Jean de Lannoy, avenue du Roi 202, B-1190 Brussels
Телефон: +32 2 538 43 08 • Факс: +32 2 538 08 41
Эл. почта: jean.de.lannoy@infoboard.be • Веб-сайт: http://www.jean-de-lannoy.be

Венгрия
Librotrade Ltd., Book Import, P.O. Box 126, H-1656 Budapest
Телефон: +36 1 257 7777 • Факс: +36 1 257 7472 • Эл. почта: books@librotrade.hu

Германия
UNO-Verlag, Vertriebs- und Verlags GmbH, August-Bebel-Allee 6, D-53175 Bonn
Телефон: +49 02 28 949 02-0 • Факс: +49 02 28 949 02-22
Эл. почта: info@uno-verlag.de • Веб-сайт: http://www.uno-verlag.de

Индия
Allied Publishers Group, 1st Floor, Dubash House, 15, J. N. Heredia Marg, Ballard Estate, Mumbai 400 001,
Телефон: +91 22 22617926/27 • Факс: +91 22 22617928
Эл. почта: alliedpl@vsnl.com • Веб-сайт: http://www.alliedpublishers.com

Bookwell, 2/72, Nirankari Colony, Delhi 110009
Телефон: +91 11 23268786, +91 11 23257264 • Факс: +91 11 23281315
Эл. почта: bookwell@vsnl.net

Испания
Díaz de Santos, S.A., c/ Juan Bravo, 3A, E-28006 Madrid
Телефон: +34 91 781 94 80 • Факс: +34 91 575 55 63 • Эл. почта: compras@diazdesantos.es
carmela@diazdesantos.es • barcelona@diazdesantos.es • julio@diazdesantos.es
Веб-сайт: http://www.diazdesantos.es

Италия
Libreria Scientifica Dott. Lucio di Biasio “AEIOU”, Via Coronelli 6, I-2 0146 Milan
Телефон: +39 02 48 95 45 52 or 48 95 45 62 • Факс: +39 02 48 95 45 48

Канада
Bernan Associates, 4611-F Assembly Drive, Lanham, MD 20706-4391, USA
Телефон: 1-800-865-3457 • Факс: 1-800-865-3450
Эл. почта: order@bernan.com • Веб-сайт: http://www.bernan.com

Renouf Publishing Company Ltd., 1-5369 Canotek Rd., Ottawa, Ontario, K1J 9J3
Телефон: +613 745 2665 • Факс: +613 745 7660
Эл. почта: order.dept@renoufbooks.com • Веб-сайт: http://www.renoufbooks.com

Китай
IAEA Publications in Chinese: China Nuclear Energy Industry Corporation, Translation Section, P.O. Box 2103, Beijing

Корея, Республика
KINS Inc., Information Business Dept. Samho Bldg. 2nd Floor, 275-1 Yang Jae-dong SeoCho-G, Seoul 137-130
Телефон: +02 589 1740 • Факс: +02 589 1746
Эл. почта: sj8142@kins.co.kr • Веб-сайт: http://www.kins.co.kr

Нидерланды
De Lindeboom Internationale Publicaties B.V., M.A. de Ruyterstraat 20A, NL-7482 BZ Haaksbergen
Телефон: +31 (0) 53 5740004 • Факс: +31 (0) 53 5729296
Эл. почта: books@delindeboom.com • Веб-сайт: http://www.delindeboom.com

Martinus Nijhoff International, Koraalrood 50, P.O. Box 1853, 2700 CZ Zoetermeer
Телефон: +31 793 684 400 • Факс: +31 793 615 698 • Эл. почта: info@nijhoff.nl • Веб-сайт: http://www.nijhoff.nl

Настоящая публикация была заменена публикацией No. 8-G (Rev. 1).

Swets and Zeitlinger B.V., P.O. Box 830, 2160 SZ Lisse
Телефон: +31 252 435 111 • Факс: +31 252 415 888 • Эл. почта: infoho@swets.nl
Веб-сайт: http://www.swets.nl

Новая Зеландия
DA Information Services, 648 Whitehorse Road, MITCHAM 3132, Australia
Телефон: +61 3 9210 7777 • Факс: +61 3 9210 7788
Эл. почта: service@dadirect.com.au • Веб-сайт: http://www.dadirect.com.au

Организация Объединенных Наций (ООН)
Dept. I004, Room DC2-0853, First Avenue at 46th Street, New York, N.Y. 10017, USA
Телефон: +800 253-9646 or +212 963-8302 • Факс: +212 963-3489
Эл. почта: publications@un.org • Веб-сайт: http://www.un.org

Словения
Cankarjeva Zalozba d.d., Kopitarjeva 2, SI-1512 Ljubljana
Телефон: +386 1 432 31 44 • Факс: +386 1 230 14 35
Эл. почта: import.books@cankarjeva-z.si • Веб-сайт: http://www.cankarjeva-z.si/uvoz

Соединенное Королевство
The Stationery Office Ltd, International Sales Agency, PO Box 29, Norwich, NR3 1 GN
Телефон (заказы): +44 870 600 5552 • (справки): +44 207 873 8372
Факс: +44 207 873 8203 • Эл. почта (заказы): book.orders@tso.co.uk
(справки): book.enquiries@tso.co.uk •Веб-сайт: http://www.tso.co.uk

Онлайновые заказы:
DELTA Int. Book Wholesalers Ltd., 39 Alexandra Road, Addlestone, Surrey, KT15 2PQ
Эл. почта: info@profbooks.com • Веб-сайт: http://www.profbooks.com

Книги по экологии:
Earthprint Ltd., P.O. Box 119, Stevenage SG1 4TP
Телефон: +44 1438748111 • Факс: +44 1438748844
Эл. почта: orders@earthprint.com • Веб-сайт: http://www.earthprint.com

Соединенные Штаты Америки
Bernan Associates, 4611-F Assembly Drive, Lanham, MD 20706-4391
Телефон: 1-800-865-3457 • Факс: 1-800-865-3450
Эл. почта: order@bernan.com • Веб-сайт: http://www.bernan.com

Renouf Publishing Company Ltd., 812 Proctor Ave., Ogdensburg, NY, 13669
Телефон: +888 551 7470 (toll-free) • Факс: +888 568 8546 (toll-free)
Эл. почта: order.dept@renoufbooks.com • Веб-сайт: http://www.renoufbooks.com

Финляндия
Akateeminen Kirjakauppa, PL 128 (Keskuskatu 1), FIN-00101 Helsinki
Телефон: +358 9 121 41 • Факс: +358 9 121 4450
Эл. почта: akatilaus@akateeminen.com • Веб-сайт: http://www.akateeminen.com

Франция
Form-Edit, 5, rue Janssen, P.O. Box 25, F-75921 Paris Cedex 19
Телефон: +33 1 42 01 49 49 • Факс: +33 1 42 01 90 90 • Эл. почта: formedit@formedit.fr

Lavoisier SAS, 14 rue de Provigny, 94236 Cachan Cedex
Телефон: + 33 1 47 40 67 00 • Факс: +33 1 47 40 67 02
Эл. почта: livres@lavoisier.fr • Веб-сайт: http://www.lavoisier.fr

Чешская Республика
Suweco CZ, S.R.O. Klecakova 347, 180 21 Praha 9
Телефон: +420 26603 5364 • Факс: +420 28482 1646
Эл. почта: nakup@suweco.cz • Веб-сайт: http://www.suweco.cz

Япония
Maruzen Company, Ltd., 13-6 Nihonbashi, 3 chome, Chuo-ku, Tokyo 103-0027
Телефон: +81 3 3275 8582 • Факс: +81 3 3275 9072
Эл. почта: journal@maruzen.co.jp • Веб-сайт: http://www.maruzen.co.jp

Заказы и запросы в отношении информации можно также направлять непосредственно по адресу:

Группа продажи и рекламы, Международное агентство по атомной энергии
Vienna International Centre, PO Box 100, 1400 Vienna, Austria
Телефон: +43 1 2600 22529 (or 22530) • Факс: +43 1 2600 29302
Эл. почта: sales.publications@iaea.org • Веб-сайт: http://www.iaea.org/books

09-36054

Настоящая публикация была заменена публикацией No. 8-G (Rev. 1).

В настоящем практическом руководстве представлена всеобъемлющая методология разработки предупредительных и защитных мер в отношении угроз ядерным установкам и операциям всех типов по перевозке ядерного материала, исходящих от внутреннего нарушителя. Внутренние нарушители, работающие в организациях и располагающие информацией о внутренних механизмах работы систем физической безопасности, это необычайно сложная задача, которую необходимо решать при создании эффективных систем контроля ядерного материала. Как правило, они обладают правами доступа, которые вместе с их полномочиями и знанием установок дают им гораздо больше возможностей в сравнении с любым внешним нарушителем для обхода специальных элементов физической защиты или других предусмотренных мер, таких, как системы безопасности и эксплуатационные процедуры. Кроме того, будучи пользующимися доверием лицами, внутренние нарушители обладают возможностями для нанесения ущерба, которыми не обладают внешние нарушители. В настоящей публикации предлагаются руководящие материалы и меры, направленные на уменьшение этих и других рисков, исходящих от внутренних нарушителей.

МЕЖДУНАРОДНОЕ АГЕНТСТВО ПО АТОМНОЙ ЭНЕРГИИ
ВЕНА
ISBN 978–92–0–411709–7
ISSN 1816–9317