Серия изданий МАГАТЭ по физической ядерной безопасности, № 23-G

Практическое руководство

Безопасность ядерной информации

IAEA
Международное агентство по атомной энергии

СЕРИЯ ИЗДАНИЙ МАГАТЭ ПО ФИЗИЧЕСКОЙ ЯДЕРНОЙ БЕЗОПАСНОСТИ

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

КАТЕГОРИИ ПУБЛИКАЦИЙ В СЕРИИ ИЗДАНИЙ МАГАТЭ ПО ФИЗИЧЕСКОЙ ЯДЕРНОЙ БЕЗОПАСНОСТИ

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

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

СОСТАВЛЕНИЕ И РЕЦЕНЗИРОВАНИЕ

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

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

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

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

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

БЕЗОПАСНОСТЬ ЯДЕРНОЙ ИНФОРМАЦИИ

Членами Международного агентства по атомной энергии являются следующие государства:

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

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

СЕРИЯ ИЗДАНИЙ МАГАТЭ ПО ФИЗИЧЕСКОЙ ЯДЕРНОЙ БЕЗОПАСНОСТИ, № 23-G

БЕЗОПАСНОСТЬ ЯДЕРНОЙ ИНФОРМАЦИИ

ПРАКТИЧЕСКОЕ РУКОВОДСТВО

МЕЖДУНАРОДНОЕ АГЕНТСТВО ПО АТОМНОЙ ЭНЕРГИИ
ВЕНА, 2023 ГОД

УВЕДОМЛЕНИЕ ОБ АВТОРСКОМ ПРАВЕ

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

Напечатано МАГАТЭ в Австрии
Июнь 2023 года
STI/PUB/1677

БЕЗОПАСНОСТЬ ЯДЕРНОЙ ИНФОРМАЦИИ
МАГАТЭ, ВЕНА, 2023 ГОД
STI/PUB/1677
ISBN 978–92–0–412922–9 (печатный формат)
ISBN 978–92–0–412822–2 (формат pdf)
ISSN 2788–8959

ПРЕДИСЛОВИЕ

Рафаэль Мариано Гросси
Генеральный директор

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

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

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

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

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

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

РЕДАКЦИОННОЕ ПРИМЕЧАНИЕ

Руководящие материалы, изданные в Серии изданий МАГАТЭ по физической ядерной безопасности, не являются обязательными для государств, однако государства могут использовать эти руководящие материалы в качестве подспорья для выполнения ими своих обязательств по международно-правовым документам, а также для осуществления ими своих обязанностей по обеспечению физической ядерной безопасности внутри государства. В тексте руководящих материалов используется формулировка «следует», отражающая международную надлежащую практику и указывающая на международный консенсус в отношении необходимости принятия государствами рекомендуемых или эквивалентных альтернативных мер.

Термины из области физической безопасности должны пониматься так, как они определены в публикации, в которой они фигурируют, или в руководящих материалах более высокого уровня, на которые опирается эта публикация. Во всех остальных случаях слова употребляются в их общепринятых значениях.

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

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

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

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

СОДЕРЖАНИЕ

1. ВВЕДЕНИЕ

ОБЩИЕ СВЕДЕНИЯ

1.1 Общая цель государственного режима физической ядерной безопасности состоит в том, чтобы защитить людей, имущество, общество и окружающую среду от вредных последствий события, связанного с физической ядерной безопасностью [1]. Группы или отдельные лица, желающие спланировать или совершить какие-либо злоумышленные действия, связанные с ядерным материалом или другим радиоактивным материалом или связанными с ними установками, могут получить доступ к чувствительной информации. Поэтому такую информацию следует идентифицировать, классифицировать и защищать с помощью соответствующих мер. Чувствительная информация — это информация в любой форме, включая программное обеспечение, несанкционированное раскрытие, корректировка, изменение, уничтожение или неиспользование которой могут поставить под угрозу физическую ядерную безопасность.

1.2 Конфиденциальность — это свойство, проявляющееся в том, что информация не предоставляется и не раскрывается лицам, структурам или процессам, не имеющим санкционированного доступа. Информационная безопасность включает в себя не только обеспечение конфиденциальности информации, но также и обеспечение точности и полноты информации (ее целостности), а также доступности или удобства использования информации по запросу (ее доступности).

1.3. Обеспечение (физической) безопасности чувствительной информации является сквозным предварительным условием обеспечения физической ядерной безопасности, и системы и меры по обеспечению эффективной информационной безопасности являются ключевыми элементами государственного режима физической ядерной безопасности.

1.4. Важность защиты чувствительной информации признается в публикации категории «Основы физической ядерной безопасности» [1] и во всех трех публикациях категории «Рекомендации по физической ядерной безопасности» [2–4]. В настоящем практическом руководстве подробно рассматриваются положения высокого уровня, содержащиеся в этих публикациях, с тем чтобы предоставить дополнительную информацию о том, что следует сделать.

ЦЕЛЬ

1.5. Настоящая публикация содержит руководящие материалы по реализации принципа конфиденциальности и по более широким аспектам информационной безопасности. Существует большое число национальных и международных руководящих материалов по созданию основ информационной безопасности для информации различных типов и управлению ими, изложенных в форме как руководящих материалов высокого уровня, так и подробных стандартов. Настоящая публикация не призвана заменить такие руководящие материалы. Вместо этого ее цель состоит в том, чтобы помочь государствам устранить пробел между существующими государственными и отраслевыми стандартами информационной безопасности в целом, конкретными концепциями и соображения, применимыми к физической ядерной безопасности, и особыми положениями и условиями, которые существуют при работе с ядерным материалом и другим радиоактивным материалом.

1.6. Целью настоящей публикации является предоставление руководящих материалов по:

a) созданию эффективной основы для обеспечения конфиденциальности, целостности и доступности чувствительной информации (раздел 3), включая необходимое законодательство и регулирующие положения;
b) выявлению информации, которая может рассматриваться как чувствительная информация (раздел 4);
c) соображениям, касающимся распространения и раскрытия чувствительной информации (раздел 5);
d) руководящим принципам и методологиям обеспечения конфиденциальности, целостности и доступности (раздел 6).

ОБЛАСТЬ ПРИМЕНЕНИЯ

1.7. В настоящей публикации рассматривается безопасность чувствительной информации для гражданского использования ядерного материала и другого радиоактивного материала и связанных с ними установок и видов деятельности. Основное внимание уделяется чувствительной информации, связанной с материалами и установками, находящимися под регулирующим контролем.

1.8. Физическая ядерная безопасность в отношении ядерного и другого радиоактивного материала, находящего вне регулирующего контроля, может также включать чувствительную информацию, безопасность которой необходимо обеспечивать. В таких случаях представленные здесь общие руководящие материалы следует применять в той мере, в которой это целесообразно.

1.9. Настоящая публикация предназначена для всех, кто несет ответственность за безопасность чувствительной информации. К ним относятся:

a) компетентные органы, включая регулирующие органы;
b) руководство на установках, в компаниях и в организациях, занимающихся использованием, хранением или перевозкой ядерного материала или другого радиоактивного материала;
c) операторы установок и их персонал, в частности сотрудники службы безопасности;
d) подрядчики или другие третьи стороны, работающие на компетентные органы, организации или операторов установок;
e) любые другие организации, которым мог быть предоставлен законный доступ к чувствительной информации.

СТРУКТУРА

1.10. После данного введения в разделе 2 приведены несколько ключевых терминов и понятий, которые будут использоваться на протяжении всей настоящей публикации. В разделе 3 описываются необходимые элементы, которые в совокупности создают основу для обеспечения безопасности чувствительной информации в государстве, а в разделах 4–6 эти элементы рассматриваются по очереди. В разделе 4 представлены соображения относительно определения того, какая информация является чувствительной и поэтому нуждается в обеспечении безопасности. Раздел 5 содержит соображения относительно обмена чувствительной информацией и ее раскрытия. Раздел 6 подробно описывает необходимые действия на уровне установки для обеспечения безопасности чувствительной информации. В Приложении I приведен пример основы классификации информации. В Приложении II приведен пример схемы категоризации информации, связанной с физической ядерной безопасностью. Предлагаемый формат и содержание программы обучения и повышения осведомленности приведены в Приложении III.

2. ПОНЯТИЯ И КОНТЕКСТ

2.1. В настоящем разделе разъясняется значение некоторых важных терминов, используемых в данной публикации. В этом разделе также применяются ключевые концепции информационной безопасности в контексте физической ядерной безопасности. Определения более широкого круга соответствующих терминов приведены в глоссарии в конце данной публикации.

ИНФОРМАЦИЯ

2.2. Информация есть знание, независимо от формы его существования или выражения. Она включает в себя идеи, понятия, события, процессы, мысли, факты и закономерности. Информация может быть записана на таких носителях, как бумага, пленка, магнитные или оптические носители, или храниться в электронных системах. Информация может представляться и передаваться практически любыми средствами. В ядерной области существует огромное количество информации во многих формах. Информационные активы — это оборудование или компоненты (включая носители), которые используются для хранения, обработки, передачи информации или управления ею.

2.3. В целях обработки и обеспечения физической безопасности информация может быть сгруппирована в информационные объекты. Их можно определить как все элементы информации, имеющие ценность для организации. Как правило, информационный объект содержит набор данных, информации или знаний, которые имеют общие использование, цель, связанный с ними риск или форму хранения или передачи.

2.4. Важно понимать, что информация, связанная с физической ядерной безопасностью, может иметь ценность (возможно, разного характера и значимости) для любого или всех следующих субъектов:

a) государства;
b) компетентных органов;
c) операторов установок (включая третьи стороны, такие как поставщики);
d) потенциальных нарушителей (отдельных лиц и организованных сообществ);

e) средств массовой информации;
f) общественности.

ВЫЯВЛЕНИЕ И ЗАЩИТА ЧУВСТВИТЕЛЬНОЙ ИНФОРМАЦИИ

2.5. Чувствительной информацией является информация, несанкционированное раскрытие (или корректировка, изменение, уничтожение или неиспользование) которой может поставить под угрозу физическую ядерную безопасность или иным образом способствовать совершению злоумышленного действия против ядерной установки, организации или перевозки. Такая информация может относиться, например, к мерам физической ядерной безопасности на установке, системам, конструкциям и элементам на установке, местонахождению и подробностям перевозки ядерного материала или другого радиоактивного материала или подробным сведениям о персонале организации.

2.6. Выявление информации, удовлетворяющей этому определению, является одним из ключевых шагов в создании программы информационной безопасности с целью обеспечения конфиденциальности. Более подробные и всесторонние руководящие материалы по данной теме представлено в разделе 4, а наглядные примеры приведены в Приложении II.

2.7. Обеспечение безопасности чувствительной информации необходимо, поскольку легкий доступ к недостаточно защищенной информации может помочь нарушителям спланировать или совершить злоумышленные действия с относительно небольшими усилиями или риском. Если, например, нарушителями, планирующими нападение на установку, был получен план физической защиты установки, то они будет знать препятствия, с которыми им придется столкнуться, численность и вооружение службы охраны, численность сил реагирования и приблизительное время прибытия сил реагирования на площадку. Они также будут знать важные цели на установке, их местонахождение и меры по их защите. Точно так же, если нарушителю, желающему похитить ядерный материал во время перевозки, удалось получить устройство, дающее доступ к подробной информации о планируемой перевозке, поскольку это устройство было недостаточно защищено, нарушитель может спланировать нападение более эффективно. Таким образом, обладание такой информацией или информационными активами нарушителями повысит вероятность их успеха.

2.8. Доступ к чувствительной информации и объектам с чувствительной информацией не следует расширять более, чем это необходимо для ведения деятельности организации. Это означает, что распространение следует ограничить кругом лиц, доступ которых должным образом санкционирован, и только теми обстоятельствами, при которых им необходим доступ. Правила «необходимо знать» и «необходимо сохранять» имеют основополагающее значение для обеспечения безопасности чувствительной информации. Этими правилами следует руководствоваться при управлении правами доступа к информации и при их контроле. Права доступа следует пересматривать периодически и по мере необходимости.

2.9. Обеспечение конфиденциальности зависит от применения мер физической безопасности к выбранной чувствительной информации и чувствительным информационным активам (оборудованию или компонентам, включая носители, которые обеспечивают обработку, хранение, передачу чувствительной информации или обращение с ней), с тем чтобы гарантировать, что они не попадут в руки посторонних, неуполномоченных лиц или организаций, как внешних так и внутренних. Руководящие материалы по мерам против внутренних угроз содержится в публикации «Предупредительные и защитные меры в отношении угроз, исходящих от внутреннего нарушителя» [5]. Меры физической безопасности следует основывать на анализе рисков. Анализ рисков следует обновлять посредством процесса периодических обзоров.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

2.10. Информационная безопасность, как описано в этой публикации, относится к системе, программе или набору правил, обеспечивающих конфиденциальность, целостность и доступность информации в любой форме. Как минимум, это включает в себя:

a) безопасность информации в физических формах (например, на бумажных и электронных носителях);
b) физическую безопасность компьютерных систем, иногда называемую компьютерной безопасностью, безопасностью информационных технологий (ИТ) или кибербезопасностью (дополнительные руководящие материалы МАГАТЭ можно найти в публикации «Компьютерная безопасность на ядерных установках» [6]);

c) физическую безопасность информационных активов (например, оборудования для хранения и обработки информации, систем и сетей связи);
d) безопасность информации о сотрудниках установки и третьих лицах (например, о подрядчиках и поставщиках), которая может поставить под угрозу безопасность перечисленного выше;
e) безопасность нематериальной информации (например, знаний).

2.11. Хотя часто выделяют конфиденциальность, организациям следует обеспечить, чтобы их программа информационной безопасности учитывала все три атрибута. Потеря целостности или доступности может негативно сказаться на физической ядерной безопасности точно так же, как и потеря конфиденциальности. Например, если законные пользователи не имеют своевременного доступа к информации, необходимой для выполнения их обязанностей (потеря доступности), или если эта информация была изменена таким образом, что вводит их в заблуждение (потеря целостности).

2.12. Информационную безопасность следует рассматривать и применять в контексте общей основы физической безопасности. Она тесно взаимозависима с другими областями физической безопасности, такими как физическая защита и безопасность персонала. Например, меры физической защиты могут использоваться для защиты чувствительной информации и чувствительных информационных активов, в то время как меры конфиденциальности делают нападение на системы физической защиты более сложным или неопределенным для нарушителей. Пробелы или недостатки в любой из областей физической безопасности могут повлиять на физическую безопасность в других областях, поэтому важно использовать комплексный подход, учитывающий все области вместе.

2.13. В информационной безопасности следует также учитывать необходимый баланс между физической безопасностью и другими целями, включая безопасность, открытость и прозрачность, а также эксплуатационные аспекты. Руководящие материалы по безопасности содержатся в публикациях Серии норм безопасности МАГАТЭ.

3. ОСНОВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ЧУВСТВИТЕЛЬНОЙ ИНФОРМАЦИИ

3.1. Обеспечение безопасности чувствительной информации на фрагментарной основе, от установки к установке, не будет эффективным. Необходима эффективная национальная основа для обеспечения комплексных мер физической безопасности на всех установках, площадках и во всех организациях (государственных и негосударственных), обрабатывающих чувствительную информацию. Государству следует создать эту национальную основу, которая будет включать установление:

a) ответственности государства;
b) правовой и регулирующей основы;
c) национальных руководящих материалов;
d) направлений политики обеспечения физической безопасности;
e) схем классификации.

Направления политики в рамках каждой организации также внося вклад в общую основу.

ОБЯЗАННОСТИ

3.2. Ответственность за обеспечение существования и эффективного функционирования всеобъемлющего режима физической ядерной безопасности государства лежит на правительстве этого государства. Обеспечение безопасности чувствительной информации является неотъемлемой частью режима физической ядерной безопасности, соблюдение которого следует обеспечивать государству.

3.3. В государствах, как правило, существуют правительственные организации или учреждения, отвечающие за общую национальную физическую безопасность, далее именуемые органами национальной безопасности. Органы национальной безопасности обычно несут ответственность за определение фундаментальной национальной политики по всем аспектам физической безопасности. Направления политики физической безопасности и инструкции, издаваемые компетентными органами национальной безопасности, часто носят общий характер и не предназначены специально для области физической ядерной безопасности. Однако компетентные органы национальной безопасности многих

государств располагают направлениями политики и руководящими материалами по обеспечению безопасности чувствительной информации, например, для использования правительством или военными.

3.4. Соответствующим компетентным органам государства следует разработать и опубликовать политику и требования, относящиеся к безопасности чувствительной информации на установках и в отношении видов деятельности, которые связаны с ядерным и другим радиоактивным материалом. Обычно они основаны на любой национальной политике и требованиях в области физической безопасности, издаваемых компетентными органами национальной безопасности, и соответствуют им, но с учетом особого характера деятельности, связанной с такими материалами. Компетентным органам также следует поддерживать тесную связь с компетентными органами национальной безопасности с целью разработки оценки национальной угрозы или проектной угрозы (дополнительную информацию см. в публикации «Development, Use and Maintenance of the Design Basis Threat» («Разработка, использование и совершенствование критериев проектной угрозы») [7]).

3.5. Каждой организации следует разработать свою внутреннюю политику, планы и процедуры для обеспечения конфиденциальности, целостности и доступности любой чувствительной информации, связанной с физической ядерной безопасностью, которую она хранит или с которой она обращается, а также для защиты связанных с ней чувствительных информационных активов согласно национальной политике в области физической безопасности и соответствующим национальным законам и требованиям. Всем сотрудникам следует полностью осознавать необходимость обеспечения информационной безопасности и соблюдать правила и процедуры информационной безопасности своей организации.

ПРАВОВАЯ И РЕГУЛИРУЮЩАЯЯ ОСНОВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ЧУВСТВИТЕЛЬНОЙ ИНФОРМАЦИИ

3.6. Требования по поддержанию физической ядерной безопасности в границах государства следует применять в отношении всех министерств, ведомств, учреждений и других организаций, занимающихся вопросами, которые государство считает необходимыми для обеспечения национальной физической ядерной безопасности. Государство может устанавливать эти требования посредством законов, регулирующих положений или других юридически обязательных требований. В требования государства

в отношении обеспечения физической ядерной безопасности следует включать требования по обеспечению информационной безопасности. Также следует предусматривать законодательство, определяющее санкции или наказания, которые будут применяться к любому лицу или организации, нарушающим такие требования по обеспечению информационной безопасности. В таком законодательстве могут иметься разделы, определяющие тяжесть отдельных видов нарушения конфиденциальности или иных атрибутов информации и соответствующие санкции.

3.7. Следует обеспечивать, чтобы полномочия компетентных органов в области регулирования позволяли им налагать обязательства на владельцев чувствительной информации. В законах, принятые с этой целью, следует предусматривать санкции или наказания за несанкционированное раскрытие информации. В законодательстве также следует предписывать государственным министерствам, ведомствам, учреждениям и другим организациям оказывать компетентным органам всю необходимую поддержку, позволяющую им выполнять свою задачу по обеспечению безопасности чувствительной информации.

ПОДГОТОВКА НАЦИОНАЛЬНЫХ РУКОВОДЯЩИХ МАТЕРИАЛОВ

3.8. В государственной политике по обеспечению безопасности информации следует определять, безопасность какого типа информации государство желает обеспечивать, и указывать, как следует это делать. Обычно это излагается в руководстве по безопасности, составленном компетентными органами национальной безопасности государства (или другим соответствующим органом). В руководстве такого рода может не содержаться прямого упоминания чувствительной информации для области физической ядерной безопасности. Однако в таком руководстве будут указаны различные классы информации с указанием уровня ее конфиденциальности и, следовательно, применяемого уровня безопасности, а также способов маркировки информационных объектов с целью обеспечения того, что уровень их конфиденциальности был очевиден.

3.9. Соответствующим компетентным органам в тесном контакте с компетентными органами национальной безопасности и при участии пользователей ядерного материала и другого радиоактивного материала следует разработать подробные руководящие материалы о том, что представляет собой чувствительная информация. Такие руководящие материалы обычно основаны на положениях любой национальной оценки

угроз, и следует обеспечивать, чтобы они соответствовали ей. В руководящих материалах этого типа, иногда называемых классификационной политикой, типы информации обычно подразделяются на ряд связанных тем с указанием относительной важности конкретной части информации и, следовательно, ее конфиденциальности и, таким образом, степени безопасности, которую необходимо применить.

3.10. На уровне организации важность конкретной информации может быть указана в плане организации по обеспечению физической безопасности, в котором следует описать, как должна быть защищена конкретная чувствительная информация в соответствии с национальным законодательством и регулирующими положениями.

НАПРАВЛЕНИЯ ПОЛИТИКИ В ОБЛАСТИ ФИЗИЧЕСКОЙ БЕЗОПАСНОСТИ

3.11. В дополнение к выпуску направлений политики в области информационной безопасности согласно национальным требованиям, компетентным органам следует выработать подробные сведения о том, как эти требования следует применять в отношении установок и видов деятельности, связанных с ядерным материалом и другим радиоактивным материалом.

3.12. Следует обеспечивать, чтобы политика государства в области физической ядерной безопасности демонстрировала приверженность обеспечению информационной безопасности. Это следует поощрять посредством выпуска и поддержания всеобъемлющей и надлежащей политики информационной безопасности, которая должна применяться в отношении всех установок и видов деятельности, связанных с ядерным и другим радиоактивным материалом, а также любых других мест, где хранится соответствующая чувствительная информация. Цель этой политики — обеспечить защиту чувствительной информации от раскрытия.

3.13. Каждой организации и установке, которые имеют дело с чувствительной информацией, следует разработать свою собственную специальную политику информационной безопасности, основанную на политике компетентных органов, где это применимо. Эту политику следует доводить до сведения всей организации в форме, актуальной, доступной и понятной предполагаемым пользователям. Раздел 6 содержит

дополнительные руководящие материалы по созданию программы менеджмента информационной безопасности, включая направления политики.

СХЕМЫ КЛАССИФИКАЦИИ ИНФОРМАЦИИ

3.14. Реализация схем информационной безопасности и связанных с ними мер контроля требует ресурсов и времени. Обеспечивать равную защиту всей информации на площадке или установке невозможно или нежелательно. Определенная информация не является чувствительной и не требует каких-либо особых мер безопасности. Даже в случае чувствительной информации разные информационные объекты могут нуждаться в разных уровнях безопасности. Поэтому важно определить, какая информация является чувствительной и какой уровень безопасности для нее требуется. Компетентным органам в каждом государстве следует определять, какая информация о ядерном материале, другом радиоактивном материале, связанных с ними установках и видах деятельности представляет собой чувствительную информацию. Что касается международных перевозок, то государству следует определить, безопасность какой информации необходимо обеспечивать, и, возможно, оно пожелает рассмотреть вопрос о достижении согласованности между государствами, участвующими в международных перевозках.

3.15. Рекомендуемый способ оценки ценности конкретного информационного актива заключается в использовании риск-ориентированного подхода с учетом ущерба и последствий, которые могут возникнуть в случае раскрытия соответствующей информации. Важно отметить, что любое раскрытие информации на одной установке может повлиять на другие установки с аналогичными информационными активами; следовательно, ущерб и последствия следует рассматривать в широком смысле в отношении последствий для физической ядерной безопасности и в других местах, а не только в одном конкретном месте. Особое внимание следует уделить накоплению информации и потенциальным точкам отказа (например, информационные активы, зависящие от одной сети или источника электроснабжения). Результаты этой оценки могут быть использованы для определения необходимого уровня безопасности, требуемого для каждого информационного объекта, в соответствии с системой классификации информации, используемой конкретным государством.

3.16. Следует создать и поддерживать национальную систему классификации для группирования информации по классам, с тем чтобы несанкционированное раскрытие любой информации в рамках определенного класса имело аналогичные последствия, и, следовательно, ко всей информации в конкретном классе следует применять аналогичные требования физической безопасности. Следует обеспечивать, чтобы это была национальная система, не относящаяся к конкретной отрасли или разработанная на одной установке. Во многих случаях государства уже используют такие системы классификации, но подобные системы могут не учитывать специфическую информацию, касающуюся физической ядерной безопасности. Эта система основана на риск-ориентированном подходе, при котором потенциальные последствия несанкционированного раскрытия информации определяют класс и соответствующие требования безопасности для такой информации.

3.17. Особое внимание следует уделять количеству категорий классификации и преимуществам, которые можно получить от их использования. Очень сложные схемы могут стать громоздкими и оказаться непрактичными, тогда как очень простые схемы могут не обеспечивать достаточно точной классификации. Кроме того, следует соблюдать осторожность при присвоении уровня классификации информационным объектам. Отнесение к более высоким уровням классификации (т. е. требование более строгой защиты, чем это действительно необходимо) может приводить к ненужным дополнительным расходам, в то время как отнесение к более низким уровням классификации может подвергнуть информацию неприемлемому риску раскрытия. Отнесение к более высоким уровням классификации также может противоречить политике прозрачности или создавать ситуацию, в которой такой уровень классификации становится менее удобным для пользователей информации.

3.18. Возможная схема классификации чувствительной информации с классами, указывающими на конфиденциальность конкретных информационных объектов, может содержать следующие уровни[1]:

а) СЕКРЕТНО;

[1] Во многих государствах существует дополнительный уровень классификации «СОВЕРШЕННО СЕКРЕТНО». Этот уровень классификации почти никогда не используется в гражданском секторе большинства государств. Как правило, он относится к военному и оружейному сектору.

b) КОНФИДЕНЦИАЛЬНО;
c) ОГРАНИЧЕННОГО ИСПОЛЬЗОВАНИЯ.

3.19. Дополнительные информационные метки могут указывать на ограничения в отношении распространения информации, вытекающие из ее классификации, такие как:

a) запрещение дальнейшего распространения;
b) распространение контролируется источником информации;
c) для служебного пользования;
d) ограниченное распространение;
e) доступно для общественного пользования.

3.20. Примеры определений уровней классификации от СЕКРЕТНО до ОГРАНИЧЕННОГО ИСПОЛЬЗОВАНИЯ приведены в Приложении I.

4. ВЫЯВЛЕНИЕ ЧУВСТВИТЕЛЬНОЙ ИНФОРМАЦИИ

4.1. Первым шагом в классификации и обеспечении безопасности информации является выявление информации, которая считается чувствительной.

4.2. Меры контроля физической безопасности следует рассматривать для информации, по крайней мере, следующих типов (которая может повлиять на физическую ядерную безопасность)[2]:

a) подробные сведения о системах физической защиты и любых других действующих мерах физической безопасности в отношении ядерного материала, другого радиоактивного материала, связанных с ними установок и видов деятельности, включая информацию о силах охраны и реагирования;
b) информация, касающаяся количества и формы используемого или хранящегося ядерного материала или другого радиоактивного материала, включая информацию об учете ядерного материала;

---

[2] Этот список не предназначен для включения всех таких возможностей, но он должен служить отправной точкой для рассмотрения.

c) информация, касающаяся количества и формы ядерного материала или другого радиоактивного материала в процессе перевозки;
d) подробные сведения о компьютерных системах, включая системы связи, производящие обработку, обращение с информацией, а также хранение или передачу информации, которая прямо или косвенно важна для обеспечения безопасности и физической безопасности;
e) планы чрезвычайных мер и планы реагирования на события, связанные с физической ядерной безопасностью;
f) личная информация о сотрудниках, поставщиках и подрядчиках;
g) оценки угроз и информация для оповещения об угрозе физической безопасности;
h) сведения о чувствительных технологиях;
i) подробная информация об уязвимостях или недостатках, относящихся к вышеуказанным темам;
j) историческая информация по любой из вышеперечисленных тем.

Некоторая из вышеуказанной информации, например личная информация, также может подпадать под действие специфических требований физической безопасности в соответствии с другими национальными законами или направлениями политики компаний.

4.3. В Приложении II содержатся примеры конкретных видов информации категорий, перечисленных в пункте 4.2, с указанием того, считаются ли они обычно конфиденциальной информацией и почему.

5. ОБМЕН ЧУВСТВИТЕЛЬНОЙ ИНФОРМАЦИЕЙ И ЕЕ РАСКРЫТИЕ

5.1. Зачастую будет возникать законная потребность в постоянном обмене чувствительной информацией, например, между соответствующими государственными учреждениями, организациями, работающими с ядерным материалом или другим радиоактивным материалом, и соответствующими компетентными органами или между различными государствами. Точно так же иногда возникает необходимость раскрытия чувствительной информации другим организациям или общественности. Как обменом, так и раскрытием следует управлять таким образом, чтобы обеспечивать, что чувствительная информация не будет непреднамеренно передана или раскрыта тем, кому не нужно ее знать.

5.2. Иногда бывает необходимо, чтобы определенная чувствительная информация была передана уполномоченным государственным органам или компаниям и организациям, которым необходимо знать эту информацию. Обмен информацией может повысить эффективность, чего не было бы, если бы разработка информации и ее обработка проводились всеми самостоятельно. Также бывают случаи, когда отказ от обмена информацией может нанести ущерб физической безопасности или ослабить общее планирование, разработку и реализацию мер физической безопасности. Кроме того, поскольку ответственность за физическую ядерную безопасность часто не возлагается исключительно на какое-либо отдельное учреждение, компанию или организацию, зачастую необходимо, чтобы информация распространялась среди тех, кто разделяет ответственность за обеспечение физической безопасности. Например, часто в интересах национальной безопасности компетентным органам необходимо передавать чувствительную информацию органам национальной безопасности и наоборот, например, информацию об изменениях в оценках угроз или о событиях, связанных с физической безопасностью, следует своевременно сообщать соответствующим сторонам, с тем чтобы сделать возможной корректировку мер физической безопасности и обмен опытом эксплуатации в качестве основы для постоянного совершенствования. Помимо соображений, связанных с физической безопасностью, обмен информацией может потребоваться для поддержки других целей, включая оценку безопасности, а также технологические и коммерческие потребности.

5.3. Следует обеспечивать, чтобы характер и масштабы обмена такой информацией были основаны в первую очередь на соблюдении национальных законов или регулирующих положений, а затем на балансе между выгодами, получаемыми от обмена, и потребностями физической безопасности. Следует обеспечивать, чтобы правила передачи информации между такими компетентными органами регламентировались процедурами физической безопасности, действующими в этом государстве. Установление общего подхода в рамках государства может гарантировать, что чувствительная информация не будет раскрыта ненадлежащим образом.

5.4. Часто также возникает необходимость обмениваться определенной информацией с другими государствами или соответствующими международными организациями. В таком случае следует заключить соглашение, гарантирующее, что безопасность чувствительной информации будет обеспечена получателем в соответствии с требованиями

владельца информации. Безопасность информации может быть обеспечена двусторонним или многосторонним договором или соглашением, определяющим, как информация будет защищена от раскрытия. В таких соглашениях обычно описываются требуемые меры защиты, которые должны применяться к чувствительной информации для различных уровней классификации в каждом государстве. В них также следует учитывать, как конкретные требования в любом отдельном государстве (например, законодательство о свободе информации, см. пункт 5.6) могут повлиять на обращение с чувствительной информацией в других государствах.

РАСКРЫТИЕ ИНФОРМАЦИИ

Необходимость раскрытия

5.5. В большинстве государств действуют законы, регулирующие безопасность информации, имеющей значение для национальных интересов. В таких законах указываются санкции, которые будут применяться в случае нарушения лицом, гражданином этого государства или каким-либо иным образом законов о конфиденциальности такой информации. Также обычно существуют законы, регулирующие доступ отдельных лиц к официальной правительственной информации. Могут существовать механизмы разрешения разногласий между правительством и другими сторонами в отношении того, какую информацию можно скрывать в целях защиты национальной безопасности.

5.6. В некоторых государствах существует законодательство о свободе информации или другие законы, которые позволяют представителям общественности запрашивать доступ к информации, находящейся в распоряжении властей. Как правило, единственной информацией, которая может быть скрыта властями, является информация тех типов, на которые распространяются определенные исключения, например информация, связанная с национальной обороной, или частная и личная информация. В ряде государств объект с информацией, имеющий классификационную маркировку, автоматически не освобождается от раскрытия.

5.7. Другие законы и регулирующие положения могут требовать раскрытия определенных типов информации, которая может включать чувствительную информацию. Одним из примеров является природоохранное законодательство, которое требует публичного представления определенной

информации. Следует обеспечивать, чтобы в таких законах допускалось исключение информации, которая может затрагивать национальную безопасность или безопасность третьих сторон.

Подготовка руководящих материалов по раскрытию информации

5.8. Следует разработать специальные руководящие материалы с целью помочь организациям и установкам принять решение о том, какая чувствительная информация может быть раскрыта. При составлении таких руководящих материалов ответственное государственное учреждение обычно консультируется с другими государственными ведомствами и соответствующими организациями. Путем определения типа информации, которая считается неприемлемой для раскрытия, эти руководящие материалы следует нацеливать на предотвращение несанкционированного раскрытия чувствительной информации (см. также Приложение II).

5.9. Государствам следует рассмотреть необходимость разработки конкретных руководящих материалов с учетом:

a) конфиденциальности определенных типов чувствительной информации в зависимости от последствий ее раскрытия;
b) того, какие виды информации могут быть раскрыты, при каких обстоятельствах, кому и какими конкретными методами;
c) условий раскрытия информации;
d) процессов рассмотрения информации на предмет ее потенциальной чувствительности перед публичным представлением, например, на презентациях на конференциях, в веб-публикациях или в технических спецификациях;
e) того, какие действия следует предпринимать в случае преднамеренного или непреднамеренного несанкционированного раскрытия чувствительной информации или другого нарушения требований информационной безопасности.

5.10. Эти руководящие материалы должны будут подлежать изменению. Происходит эволюция обстоятельств и информация, которая может считаться чувствительной и непригодной для раскрытия в какой-то момент, может оказаться значительно менее чувствительной и пригодной для раскрытия впоследствии (или наоборот). Поэтому эти руководящие материалы следует рассматривать и обновлять периодически и в случае значительных изменений политики или обстоятельств.

5.11. Снижение уровня безопасности, применяемого к конкретной информации, там, где это уместно, обычно будет возможно. Однако отнесение информации к классу более ограниченного использования может оказаться невозможным или неэффективным, если она уже была раскрыта более широко. Это следует учитывать при первоначальной классификации и следует рассмотреть вопрос о надлежащем балансе между конфиденциальностью и осторожностью, с одной стороны, и доступностью и прозрачностью, с другой. Следует установить временные рамки по умолчанию для периодического рассмотрения классификаций информации, но при необходимости следует также вносить изменения, например, если обстоятельства значительно меняются.

5.12. Все запросы к организации о раскрытии чувствительной информации следует рассматривать в соответствии с одними и теми же руководящими материалами или критериями, и, если возможно, все такие запросы следует обрабатывать через единый центральный офис организации. Метод, обычно используемый для получения несанкционированного доступа к чувствительной информации, состоит в том, чтобы сделать несколько запросов к разным лицам или подразделениям в одной и той же организации. Если эти запросы рассматриваются по отдельности, без координации, могут быть даны разные ответы и может быть раскрыта чувствительная информация, которая в противном случае не была бы раскрыта.

6. ОСНОВА МЕНЕДЖМЕНТА КОНФИДЕНЦИАЛЬНОСТИ

6.1. Раздел 3 описывает основу высокого уровня для обеспечения безопасности чувствительной информации. В настоящем разделе более подробно рассматриваются компоненты такой основы, необходимые для учреждения или организации, в контексте системы менеджмента конфиденциальности.

6.2. Должна существовать система менеджмента, устанавливающая направления политики и цели и позволяющая достигать целей эффективным и действенным образом. Интегрированная система менеджмента (см. публикацию Серии норм безопасности МАГАТЭ, № GS-R-3, «Система управления объектами и деятельностью» [8] и связанные с ней руководящие материалы) является жизненно важным вспомогательным

элементом культуры физической ядерной безопасности. Многие виды деятельности на установках контролируются системами менеджмента. Они идеально объединяют элементы физической безопасности, безопасности, здравоохранения, охраны окружающей среды, качества и экономические элементы в единый процесс менеджмента или набор интегрированных и взаимоусиливающих систем. Информационную безопасность следует интегрировать в существующую систему менеджмента установки или организации с целью обеспечения конфиденциальности, целостности и доступности информации.

6.3. Обеспечение конфиденциальности, целостности и доступности чувствительной информации зависит от эффективного распределения функций и обязанностей, классификации с целью определения того, какая информация является чувствительной и нуждается в обеспечении безопасности, почему необходимо обеспечивать ее безопасность и на каком уровне (см. раздел 4), решений по способам обеспечения безопасности такой информации, реализации необходимых мер физической безопасности и реагирования (включая восстановление), если такая информация раскрыта, похищена или утрачена.

6.4. Основа менеджмента, описанная ниже, применима ко всем уровням менеджмента в организациях, хранящих чувствительную информацию или обрабатывающих ее.

ОБЯЗАННОСТИ

6.5. Руководство несет общую ответственность за обеспечение информационной безопасности и ее эффективность на всей установке или в организации с целью обеспечения безопасности чувствительной информации. Весь персонал, работающий с чувствительной информацией, несет ответственность за обеспечение ее безопасности в соответствии с соответствующим национальным законодательством, а также направлениями политики и процедурами организации.

Обязанности руководства

6.6. Обязанности руководства обычно включают:

a) принятие на себя общей ответственности за обеспечение безопасности чувствительной информации и чувствительных информационных активов;
b) обеспечение соблюдения соответствующих законов и регулирующих положений;
c) распределение организационных обязанностей по обеспечению физической безопасности;
d) обеспечение эффективной подготовки и обучения в области физической безопасности;
e) обеспечение разработки эффективной политики информационной безопасности;
f) предоставление надлежащих ресурсов для реализации эффективной программы информационной безопасности;
g) обеспечение разработки программы информационной безопасности и связанных с ней планов и процедур;
h) обеспечение эффективного управления изменениями, связанными с планами, процедурами и направлениями политики;
i) обеспечение периодических проверок, рассмотрений и пересмотров политики и процедур информационной безопасности.

Обязанности по классификации

6.7. Соответствующим компетентным органам следует предоставлять руководящие материалы по классификации, применяемой к информационному объекту, в форме руководства или руководящих материалов по классификации. В таком документе информация сгруппирована по определенным темам и указывается чувствительность этой информации. Тем, кто создает чувствительную информацию, следует использовать такое руководство при выборе соответствующего уровня классификации информации.

6.8. После распространения информации получателю или владельцу объекта чувствительной информации не следует изменять уровень классификации, применяемый к информации, без разрешения составителя. Получатели и владельцы копий могут оспаривать применяемый уровень классификации и, когда уместно, им следует делать это. Например, если компетентный орган получил от оператора информацию, которая

была неправильно классифицирована в соответствии с действующим законодательством, ему следует дать указание оператору изменить классификацию.

6.9. В тех случаях, когда организация составителя прекратила свою деятельность, ответственность ложится на ее правопреемника. Если правопреемника отследить невозможно, владелец объекта чувствительной информации может, при необходимости, изменить уровень его классификации после консультации с соответствующими компетентными органами.

6.10. Если уровень классификации, применяемый к информационному объекту, или тип информационных объектов изменяется, то об этом изменении следует уведомить, насколько это возможно, всех, кого это может затронуть. Сюда могут входить нынешние и прошлые владельцы информации, а также те, кто может использовать ее в будущем.

ПЛАН ОБЕСПЕЧЕНИЯ ФИЗИЧЕСКОЙ БЕЗОПАСНОСТИ

6.11. Всем организациям, работающим с чувствительной информацией, следует иметь план обеспечения физической безопасности. В плане обеспечения физической безопасности следует предусмотреть подробный раздел, посвященный безопасности чувствительной информации. Соответствующие требования плана обеспечения физической безопасности следует доводить до сведения сотрудников и подрядчиков, работающих в организации. Важно, чтобы сотрудники и подрядчики понимали свои обязанности.

ПОЛИТИКА И ПРОЦЕДУРЫ ОБЕСПЕЧЕНИЯ ФИЗИЧЕСКОЙ БЕЗОПАСНОСТИ

План обеспечения информационной безопасности

6.12. Ответственность за информационную безопасность следует включать в иерархию направлений политики и процедур организации. Как минимум, следует освещать указанные ниже вопросы:

а) определение информационной безопасности и изложение ее общих целей, области применения и важности;

b) определение функций и обязанностей, включая создание координационного центра с целью руководства и управления информационной безопасностью;
c) соблюдение требований информационной безопасности, включая юридические, регулирующие и договорные требования;
d) разработка плана управления рисками с целью снижения рисков до приемлемого уровня, установленного государством, путем применения надлежащих мер контроля на основе подхода, базирующегося на оценке рисков. В случае ядерной установки следует обеспечивать, чтобы план управления рисками был одобрен компетентным органом или другим органом, назначенным государством;
e) регулярный мониторинг и рассмотрение действующих механизмов с целью обеспечения того, чтобы политика, стандарты и процедуры оставались актуальными и эффективными;
f) требования к образованию и обучению с целью обеспечения того, чтобы сотрудники, подрядчики и другой персонал были должным образом осведомлены о политике, процедурах и практике в той мере, в какой это необходимо для исполнения их должностных обязанностей, и чтобы они полностью понимали свои обязанности (включая свои юридические обязательства);
g) последствия (т.е. штрафы или санкции) в случае несоблюдения требований информационной безопасности или умышленной небрежности при обеспечении безопасности чувствительной информации;
h) определение справочной документации, поддерживающей политику, например, более подробные процедуры для конкретных систем или правила физической безопасности, которых следует придерживаться пользователям.

Аспекты плана обеспечения информационной безопасности, специфичные для чувствительной информации

6.13. В плане обеспечения информационной безопасности с конкретным учетом необходимости обеспечения безопасности чувствительной информации следует также охватывать:

a) жизненный цикл информации: определение процессов создания, идентификации, классификации, маркировки, обработки, использования, хранения, передачи, переклассификации, воспроизведения и уничтожения чувствительной информации;

b) требования безопасности для чувствительной информации с учетом целей обеспечения безопасности в отношении конфиденциальности, целостности и доступности информации;
c) ограничение доступа к чувствительной информации и чувствительным информационным активам кругом тех, кто нуждается в таком доступе для выполнения своих должностных обязанностей, кто обладает необходимыми полномочиями и кто прошел проверку на благонадежность, соответствующую уровню секретности информации;
d) передачу чувствительной информации способом, который снижает до приемлемого уровня любой риск ее раскрытия, несанкционированного перехвата, изменения или нарушения.

Процедуры обращения с чувствительной информацией

6.14. Эффективное управление рисками, связанными с угрозами конфиденциальности, целостности и доступности информации, будет включать разработку эффективных контрмер против таких угроз. Этот процесс обязательно будет включать в себя комбинацию мер контроля физической безопасности, основанных на информационной безопасности, физической защите и безопасности персонала.

6.15. Проверки персонала по линии безопасности, включая проверки благонадежности, гарантируют, что те, кто имеет доступ к чувствительной информации, будут считаться государством достаточно благонадежными для этого. В случае информации относительно низкой категории секретности организации следует решить, нужны ли какие-либо проверки тех, кому требуется доступ; в этом случае может быть достаточно ограниченной проверки анкетных данных сотрудника. Для доступа к информации более высокой категории секретности потребуется более полный набор проверок анкетных данных с целью определения благонадежности. Процесс обеспечения кадровой безопасности также должен включать в себя заключение соглашения о неразглашении между лицом и компетентным органом или соответствующей организацией.

6.16. Физическая защита часто сочетает определенную степень строго регулируемого доступа через безопасный периметр с одним или несколькими уровнями других мер физической защиты ближе к информационным активам, например хранилищам и другим защищенным местам. Те же принципы можно использовать для обеспечения физической защиты информации и информационных активов.

6.17. Меры информационной безопасности включают технические, процедурные и административные меры контроля, применяемые на протяжении всего жизненного цикла информационных объектов, включая создание, обработку, хранение, передачу, тиражирование и уничтожение. Меры информационной безопасности включают, в частности:

a) административный менеджмент для управления, поддержания и развития информационной безопасности (включая услуги третьих сторон);
b) кадровую безопасность, особенно на этапах найма, а также в начале и в конце трудовой деятельности;
c) физическую безопасность зон, где используется, обрабатывается или находится чувствительная информация или чувствительные информационные активы;
d) безопасность цифровой и ручной обработки информации: физическую безопасность рабочих станций, защиту от вирусов и вредоносных программ, удаление и уничтожение информации и защиту ручных процессов;
e) физическую безопасность коммуникационных сетей (телефоны, электронная почта, Интернет и локальные сети): политика, аутентификация пользователей, идентификация оборудования, разделение, управление подключением и маршрутизацией, а также мониторинг;
f) физическую безопасность оборудования: контроль доступа, регистрация использования, управление запасными частями, резервирование критически важного оборудования, организация резервного питания, документация и техническое обслуживание, безопасность кабелей и носителей;
g) безопасность программного обеспечения: контроль доступа, регистрация действий пользователей и суперпользователей (администраторов), управление резервным копированием, заключение контрактов на техническое обслуживание, управление конфигурацией и версиями, использование зарегистрированного легального программного обеспечения, тестирование на уязвимости и тестирование поведения системы в условиях ошибки;
h) безопасность использования информационных систем: контроль прав пользователей, распознавание и проверка пользователей, подключение к службам, системам и оборудованию, управление паролями, надзор за использованием и правило двух лиц (т.е. контроль двумя лицами) в случае важнейших операций;

i) классификацию и соответствующие процедуры обработки информации;
j) защиту частной жизни.

6.18. Обращение с чувствительной информацией следует регулировать с помощью процедур в соответствии с разделом по информационной безопасности национальной политики и руководящих материалов по обеспечению физической безопасности, включая любое их толкование компетентными органами государства. В плане обеспечения информационной безопасности следует изложить минимальные эксплуатационные стандарты для различных уровней безопасности. Примером может служить методология шифрования, используемая для электронной передачи информации.

Система менеджмента прав

6.19. Следует предусмотреть систему менеджмента, устанавливающую контроль над тем, как, почему и когда конкретные держателям и пользователям чувствительной информации следует выдавать официальное разрешение на доступ к чувствительной информации и чувствительной информационным активам. Система менеджмента прав обычно включает:

a) определенную структуру ответственности в отношении менеджмента авторизации;
b) определенные процессы в отношении функции, кто имеет право кого назначать, и кто имеет право доступа к чувствительной информации и чувствительным информационным активам;
c) определенные процессы проверки, контроля и надзора за функцией предоставления доступа;
d) определенные процессы для определения того, как долго должно действовать официальное разрешение на доступ к чувствительной информации и чувствительным информационным активам;
e) определенные процессы для отзыва официального разрешения на доступ к чувствительной информации и чувствительным информационным активам;
f) определенные процессы для обеспечения полной прослеживаемости менеджмента прав на всех этапах цепочки менеджмента выдачи официальных разрешений на доступ к чувствительной информации и чувствительным информационным активам.

Периодические рассмотрения

6.20. Следует обеспечивать эволюцию направлений политики, планов и процедур физической безопасности в соответствии с изменяющимися обстоятельствами. Эффективным способом обеспечения их актуальности может быть включение временны*ы*х рамок рассмотрения в сам документ о политике. В случае фундаментального изменения обстоятельств, которое может привести к изменению политики, например, к изменению законодательства, рассмотрение может проводиться ранее. Структуру рассмотрения следует применять в отношении политики на всех уровнях обязанностей по обеспечению физической ядерной безопасности.

КУЛЬТУРА ФИЗИЧЕСКОЙ БЕЗОПАСНОСТИ

6.21. Развитие, укрепление и поддержание надежной культуры физической ядерной безопасности является важным элементом режима физической ядерной безопасности. Это особенно верно в отношении информационной безопасности, в которой люди и процессы часто являются ключевым фактором в обеспечении безопасности информации.

6.22. В рамках эффективной культуры физической ядерной безопасности [9] всем организациям, сотрудникам и подрядчикам следует иметь полное представление о своих обязанностях по обеспечению физической безопасности и важности этих обязанностей. Крайне важно, чтобы сотрудники и подрядчики получали образование и подготовку по вопросам физической безопасности в соответствии с их индивидуальными обязанностями и потребностями.

6.23. Сотрудники и подрядчики с особыми обязанностями по обеспечению физической безопасности и лица, имеющие доступ к чувствительной информации, а также руководство на всех уровнях организации нуждаются в специальном обучении и инструктаже относительно своих обязанностей. Также важно обеспечивать, чтобы другие категории сотрудников (например, курьеры, сотрудники службы безопасности и конторские служащие), которые работают с чувствительной информацией, не обязательно зная о ее содержании, также проходили обучение по вопросам физической безопасности, относящееся к их обязанностям.

6.24. Разовые учебные мероприятия по информационной безопасности не будут надлежащим образом подкреплять обучение и могут в долгосрочной перспективе приводить к возникновению у сотрудников самоуспокоенности. Всем, кто имеет дело с чувствительной информацией, включая все руководство, сотрудников и подрядчиков, следует проходить постоянное обучение на рабочем месте и посещать периодические курсы повышения квалификации. Следует вести записи об официальном обучении, полученном и завершенном всеми сотрудниками и подрядчиками. Особенно важно, чтобы любые изменения правил и процедур физической безопасности были доведены до сведения всех соответствующих сотрудников и подрядчиков как можно скорее. Предлагаемый формат и содержание программы обучения и повышения осведомленности приведены в Приложении III.

ДОГОВОРЕННОСТИ С ТРЕТЬИМИ ЛИЦАМИ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

6.25. Компетентному органу или организации иногда требуется третья сторона для предоставления услуг или товаров, связанных с чувствительной информацией. Подобные договоренности следует заключать посредством юридических соглашений, таких как лицензия или контракт, включая соглашения о неразглашении. Такие соглашения с третьими сторонами могут предусматривать передачу чувствительной информации третьим лицам. Для обеспечения того, чтобы такая информация не подвергалась риску, следует предусмотреть национальную политику или законодательство, регулирующее договоренности, касающиеся чувствительной информации. В этом случае договаривающимся организациям и установкам следует быть обязанными соблюдать эту политику.

6.26. При ведении переговоров о таких отношениях с третьими сторонами договаривающиеся организации обязаны обеспечивать, чтобы любая чувствительная информация, доверенная третьим сторонам, была удовлетворительным образом защищена. Следует обеспечивать, чтобы меры физической безопасности с целью защиты чувствительной информации были соразмерны рискам и соответствовали политике.

6.27. В этом контексте компетентным органам и организациям следует убедиться, что третьи стороны:

a) располагают процессами и процедурами информационной безопасности, которые отвечают, по крайней мере, требованиям собственных мер физической безопасности организации;
b) располагают координационным центром для руководства и управления физической безопасностью в подрядной компании;
c) внедрили систему, гарантирующую, что все сотрудники, имеющие доступ к чувствительной информации, которой владеет третья сторона, проходят проверку на благонадежность на соответствующем уровне;
d) обеспечивают, что доступ к чувствительной информации и чувствительным информационным активам предоставляется только тем, у кому это необходимо знать и тем, кто имеет надлежащий уровень допуска;
e) передают информацию в соответствии с национальным законодательством, местной политикой и таким образом, чтобы информация не подвергалась риску раскрытия;
f) гарантируют, что информация не будет передана какой-либо неуполномоченной стороне или лицу;
g) обеспечивают, чтобы весь персонал был надлежащим образом осведомлен о политике и практике обеспечения физической безопасности и полностью понимал свои обязанности (включая свои юридические обязательства);
h) располагают процедурами реагирования на события, связанные с информационной безопасностью;
i) обеспечивают, чтобы меры физической безопасности в помещениях третьей стороны регулярно инспектировались компетентными органами или подрядными организациями в соответствии с положениями соглашения, с тем чтобы убедиться, что они соответствуют требованиям физической безопасности, изложенным в соглашении.

ИНСПЕКЦИИ И АУДИТЫ

6.28. Регулярное осуществление деятельности по обеспечению физической безопасности имеет важное значение для поддержания программы информационной безопасности. Необходима уверенность в том, что программы физической безопасности, действующие в организациях,

владеющих чувствительной информацией, включая третьи стороны, во всех аспектах соответствуют национальной политике и регулирующим положениям. В надлежащих случаях компетентным органам следует рассматривать меры информационной безопасности до того, как будет предоставлено официальное разрешение на их использование. Уверенность может быть достигнута путем проведения регулярных официальных инспекций или аудитов организации или установки. Аудиты обычно проводятся в рамках организации, тогда как инспекции могут носить как внутренний, так и внешний характер. Кроме того, инспекции могут быть как объявленными, так и необъявленными (т.е. с предварительным уведомлением или без него).

6.29. Внутренние инспекции и аудиты проводятся организацией для определения того, соответствует ли действующая программа физической безопасности одобренному плану обеспечения информационной безопасности, и для обеспечения соблюдения регулирующих положений. Такие инспекции позволяют организации проверять собственное соблюдение с большей частотой, чем внешние инспекции. Кроме того, инспекции или аудиты, проводимые персоналом, знакомым с внутренними требованиями, процедурами и системами, могут выявить возможности для улучшения, которые отличаются от тех, которые могут быть обнаружены при внешней инспекции.

6.30. К внешним инспекциям относятся инспекции, проводимые компетентными органами или другими уполномоченными сторонними организациями. Целью таких инспекций является оценка уровня соблюдения государственной политики в области информационной безопасности. Внешние инспекции обеспечивают независимую оценку по сравнению с инспекциями, проводимыми самой организацией. При использовании внешних аудиторов следует решать вопросы конфиденциальности и их благонадежности.

6.31. В результатах инспекций и аудитов следует выделять конкретные области, требующие принятия мер или улучшений. Для выявленных профилактических и корректирующих мер следует указывать конкретные временны*е* рамки устранения недостатков или реализации. Следует отслеживать принятие мер по исправлению и реализации и оценивать их эффективность.

ИНЦИДЕНТЫ, СВЯЗАННЫЕ С ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

6.32. Нарушения безопасности могут быть результатом раскрытия содержания информационного объекта. Два типа нарушений, при которых происходит раскрытие содержания информации, — это утечки и потери. Утечки обычно связаны с нарушением конфиденциальности, когда имело место несанкционированное раскрытие информации, преднамеренное или случайное. Потери, как правило, связаны с раскрытием содержания информации в результате хищения или неспособности обеспечить надлежащую безопасность информации или информационных активов.

6.33. Инциденты, связанные с информационной безопасностью, могут также включать потерю доступности или целостности информации, которая может произойти непреднамеренно или в результате преднамеренных действий. Потеря доступности может произойти, например, из-за сбоя в информационной системе (такой как база данных) или злонамеренного отказа в использовании (преднамеренного глушения информационной сети чрезмерным трафиком данных). Потеря целостности может быть вызвана, например, повреждением информационной системы, повреждением базы данных или несанкционированным изменением информации во время передачи.

6.34. Представление компетентным органам отчетов о значительных инцидентах, связанных с физической ядерной безопасностью, или нарушениях физической ядерной безопасности, включая нарушения информационной безопасности, следует сделать обязательным, и это требование следует закрепить в законах или регулирующих положениях государства. В законах или регулирующих положениях также следует указывать санкции или штрафы за непредставление таких отчетов.

6.35. Руководителям организаций и установок следует обеспечивать наличие официальных механизмов отчетности для обеспечения того, чтобы информация о всех инцидентах, связанных с информационной безопасностью, немедленно доводилась до их сведения, с тем чтобы можно было предпринять корректирующие меры и, при необходимости, сообщить об инциденте компетентным органам. Смущение не следует делать причиной отказа сообщить о каком-либо инциденте, связанном с информационной безопасностью, на любом уровне. Об инцидентах следует сообщать незамедлительно, с тем чтобы можно было предпринять соответствующие корректирующие меры и выявить тенденции.

РАССЛЕДОВАНИЯ

6.36 Все инциденты, связанные с информационной безопасностью, следует подвергать расследованию. Следует определить направления политики и процедуры, регулирующие расследование инцидентов, связанных с информационной безопасностью. Целью расследования следует делать определение того, оказывает ли инцидент, связанный с физической безопасностью, незначительное или значительное влияние на информационную безопасность и конфиденциальность. Затем компетентные органы могут инициировать любые соответствующие действия. Примером незначительного инцидента может служить ненадлежащее хранение или ненадлежащее обеспечение сохранности документа, которое не привело к потере или раскрытию содержания какой-либо информации. Серьезным инцидентом, например, может быть хищение плана обеспечения физической безопасности, создающее стратегическую угрозу для организации.

6.37. При проведении расследования следует:

a) полностью изучить обстоятельства инцидента, с тем чтобы установить его масштабы, размах и воздействие;
b) оценить последствия инцидента и степень раскрытия содержания информации, которая могла иметь место;
c) оценить необходимость принятия дальнейших мер или проведения более широких расследований, возможно, с привлечением других учреждений;
d) рекомендовать корректирующие меры или принять меры с целью локализации или сведения к минимуму последствий;
e) сообщить о результатах расследования, включая указание:
   i) вероятной причины инцидента;
   ii) оцененной степени раскрытия содержания информации;
   iii) вероятных последствий раскрытия содержания информации;
   iv) возможных рекомендаций по улучшению программы обеспечения физической безопасности во избежание повторения подобного инцидента;
   v) рекомендуемых дальнейших действий, оправданных в связи с инцидентом;
   vi) уроков, которые необходимо усвоить заинтересованным сторонам.

6.38. Компетентным органам следует вести записи о количестве и типе зарегистрированных инцидентов, связанных с информационной безопасностью. Следует идентифицировать повторяющиеся инциденты или

тенденции сбоев в обеспечении физической безопасности, которые могут указывать на необходимость внесения изменений в политику физической безопасности или усовершенствований в процедурах или программах обеспечения физической безопасности. Обновленную информацию о тенденциях и изменениях также следует включать в обучение по повышению осведомленности, с тем чтобы поддерживать соответствующую культуру физической безопасности среди сотрудников и подрядчиков. Организациям и учреждениям также следует вести свои собственные записи.

СПРАВОЧНЫЕ МАТЕРИАЛЫ

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

[2] МЕЖДУНАРОДНОЕ АГЕНТСТВО ПО АТОМНОЙ ЭНЕРГИИ, Рекомендации по физической ядерной безопасности по физической защите ядерного материала и ядерных установок (INFCIRC/225/Revision 5), Серия изданий МАГАТЭ по ядерной безопасности, № 13, МАГАТЭ, Вена (2011).

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

[4] ВСЕМИРНАЯ ТАМОЖЕННАЯ ОРГАНИЗАЦИЯ, ЕВРОПЕЙСКОЕ ПОЛИЦЕЙСКОЕ УПРАВЛЕНИЕ, МЕЖДУНАРОДНАЯ ОРГАНИЗАЦИЯ ГРАЖДАНСКОЙ АВИАЦИИ, МЕЖДУНАРОДНАЯ ОРГАНИЗАЦИЯ УГОЛОВНОЙ ПОЛИЦИИ — ИНТЕРПОЛ, МЕЖДУНАРОДНОЕ АГЕНТСТВО ПО АТОМНОЙ ЭНЕРГИИ, МЕЖРЕГИОНАЛЬНЫЙ НАУЧНО-ИССЛЕДОВАТЕЛЬСКИЙ ИНСТИТУТ ОРГАНИЗАЦИИ ОБЪЕДИНЕННЫХ НАЦИЙ ПО ВОПРОСАМ ПРЕСТУПНОСТИ И ПРАВОСУДИЯ, УПРАВЛЕНИЕ ОРГАНИЗАЦИИ ОБЪЕДИНЕННЫХ НАЦИЙ ПО НАРКОТИКАМ И ПРЕСТУПНОСТИ, Рекомендации по физической ядерной безопасности, касающиеся ядерных и других радиоактивных материалов, находящихся вне регулирующего контроля, Серия изданий МАГАТЭ по ядерной безопасности, № 15 МАГАТЭ, Вена (2011).

[5] МЕЖДУНАРОДНОЕ АГЕНТСТВО ПО АТОМНОЙ ЭНЕРГИИ, Предупредительные и защитные меры в отношении угроз, исходящих от внутреннего нарушителя, Серия изданий МАГАТЭ по ядерной безопасности, № 8, МАГАТЭ, Вена (2009).

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

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

[8] МЕЖДУНАРОДНОЕ АГЕНТСТВО ПО АТОМНОЙ ЭНЕРГИИ, Система управления для установок и деятельности, Серия норм безопасности МАГАТЭ, № GS-R-3, МАГАТЭ, Вена (2008).

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

Приложение I

СИСТЕМА КЛАССИФИКАЦИИ И ОПРЕДЕЛЕНИЯ

I–1. В приложении I приведен пример основы классификации. Отдельные государства могут разработать и использовать любую соответствующую систему классификации для указания уровня чувствительности информации о физической ядерной безопасности. Приведенные ниже определения представляют собой четырехуровневую систему, аналогичную той, что используется во многих государствах-членах МАГАТЭ. Четвертый уровень «СОВЕРШЕННО СЕКРЕТНО» не обсуждается, поскольку опыт показывает, что в области гражданской ядерной энергетики весьма маловероятно, что какие-либо информационные активы будут подпадать под гриф «СОВЕРШЕННО СЕКРЕТНО». Следует также отметить, что, хотя информация, как предполагается, представлена главным образом в форме документов или знаний, элементы оборудования или другие физические объекты могут быть также классифицированы, если чувствительная информация может быть получена путем визуального наблюдения за их внутренним или внешним видом, структурой, работой, испытаниями, применением или использованием.

СЕКРЕТНО

I–2. Раскрытие информации или материалов, классифицированных грифом СЕКРЕТНО, вероятно, может:

a) усилить международную напряженность;
b) нанести серьезный ущерб отношениям между правительствами;
c) создать прямую угрозу жизни или нанести серьезный ущерб общественному порядку, личной безопасности или свободе;
d) причинить серьезный ущерб эффективности оперативных действий или безопасности национальных сил безопасности или сохранению эффективности важных операций по обеспечению безопасности или разведывательных операций;
e) нанести существенный материальный ущерб национальным финансам или экономическим и коммерческим интересам;
f) использоваться лицом или группой лиц, планирующих злоумышленное действие, которое может нанести серьезный ущерб установке с ядерным или другим радиоактивным материалом или во время перевозки такого материала.

КОНФИДЕНЦИАЛЬНО

I–3. Раскрытие информации или материалов, классифицированных грифом КОНФИДЕНЦИАЛЬНО, вероятно, может:

a) нанести ущерб дипломатическим отношениям;
b) нанести ущерб личной безопасности или свободе;
c) нанести ущерб эффективности оперативных действий или безопасности национальных сил безопасности или эффективности важных операций по обеспечению безопасности или разведывательных операций;
d) в значительной степени работать против национальных финансов или экономических и коммерческих интересов;
e) существенно подорвать финансовую жизнеспособность крупных организаций;
f) препятствовать расследованию или способствовать совершению тяжких преступлений;
g) серьезно препятствовать разработке или реализации основных направлений государственной политики;
h) остановить или иным образом существенно нарушить важные государственные операции;
i) использоваться лицом или группой лиц, планирующих злоумышленное действие, которое может нанести серьезный ущерб установке с ядерным материалом или другим радиоактивным материалом или во время перевозки такого материала.

ОГРАНИЧЕННОГО РАСПРОСТРАНЕНИЯ

I–4. Раскрытие информации или материалов, классифицированных грифом ОГРАНИЧЕННОГО РАСПРОСТРАНЕНИЯ, вероятно, может:

a) неблагоприятно повлиять на дипломатические отношения;
b) причинить существенный вред отдельным лицам;
c) затруднить поддержание операционной эффективности или безопасности национальных сил безопасности;
d) причинить финансовые убытки или сформировать условия для потенциальной потери заработка, содействовать неправомерной выгоде или преимуществам для отдельных лиц или компаний;
e) препятствовать расследованию преступления;
f) облегчить совершение преступления;

g) нарушить надлежащие обязательства по сохранению конфиденциальности информации, предоставленной третьими сторонами;
h) препятствовать эффективной разработке или осуществлению направлений государственной политики;
i) нарушить установленные законом ограничения на раскрытие информации;
j) ставить правительство в невыгодное положение в коммерческих или политических переговорах с другими сторонами;
k) подорвать надлежащее управление государственным сектором и его операциями;
l) использоваться лицом или группой лиц, планирующих злоумышленное действие, которое может причинить значительный ущерб на установке с ядерным материалом или другим радиоактивным материалом или во время перевозки такого материала.

I–5. Что касается применения вышеуказанных уровней классификации в отношении контроля чувствительной ядерной информации, то следует рассмотреть вопрос о том, как несанкционированное раскрытие такой информации может помочь потенциальному нарушителю в следующем:

a) выбор цели для акта хищения или саботажа (диверсии) с использованием ядерного материала или другого радиоактивного материала, оборудования или установок;
b) планирование или совершение акта хищения или саботажа (диверсии) в отношении ядерного материала или другого радиоактивного материала, оборудования или установок с использованием:
    i) данных о проектировании систем безопасности;
    ii) планов строительства;
    iii) методов и процедур передачи, учета ядерного или другого радиоактивного материала и обращения с ним;
    iv) планов, процедур и возможностей обеспечения безопасности;
c) оценка успеха акта хищения или саботажа (диверсии) в отношении ядерного материала или другого радиоактивного материала, оборудования или установок, с учетом следующих знаний:
    i) фактические или гипотетические последствия саботажа (диверсии) в отношении конкретного жизненно важного оборудования или установок;

d) незаконное изготовление ядерного взрывного устройства, радиологического диспергирующего устройства или радиационного облучающего устройства с учетом следующих знаний:
   i) информация о конструкции такого устройства, полезная при его разработке;
   ii) местонахождение материалов, необходимых для изготовления устройства;
   iii) местонахождение ядерного оружия;
e) рассеивание ядерного материала или другого радиоактивного материала в окружающей среде:
   i) расположение, форма и количество материалов.

Приложение II

ПРИМЕРЫ ЧУВСТВИТЕЛЬНОЙ ИНФОРМАЦИИ

II–1. В Приложении II приведен пример схемы категоризации безопасности информации, связанной с физической ядерной безопасностью. Государству следует определить точный уровень классификации, который будет применяться к каждому элементу такой информации. В Таблице II–1 приведены примеры чувствительной информации и указаны связанные с ними вопросы конфиденциальности. В тех случаях, когда разглашение информации не рекомендуется, в этой таблице указаны причины обеспечения физической безопасности и может ли оно быть оправдано.

II–2. Категории информации, представленные в Таблице II–1 , являются лишь ориентировочными в отношении того, что может считаться чувствительной информацией. Они не предназначены для использования в качестве исчерпывающего списка или модели. Актуальность категорий, подлежащих включению в любую аналогичную таблицу государственной классификации, будет определяться в соответствии с конкретной оценкой государства.

II–3. В каждой строке таблицы первый столбец описывает примерный тип информации. Во втором столбце указано, применима ли эта категория обычно к ядерному материалу и ядерным установкам (N), другому радиоактивному материалу и связанным с ними установкам (R) или к обоим (N, R). В третьем столбце указано, можно ли считать информацию чувствительной или не чувствительной. В последнем столбце дается объяснение чувствительности информации и обоснование обеспечения ее безопасности.

II–4. При определении информации как чувствительной и присвоения соответствующего уровня конфиденциальности следует учитывать связанную информацию, которая уже появилась в открытом доступе, любое предыдущее раскрытие или возможное раскрытие информации. Присваивать уровень конфиденциальности такой информации и управлять им может оказаться нецелесообразным.

II–5. Следует также рассмотреть возможность обозначения якобы нечувствительной информации как чувствительной, если она в сочетании с другой нечувствительной информацией может быть использована для раскрытия чувствительной информации.

ТАБЛИЦА II–1. УСЛОВНАЯ СХЕМА КАТЕГОРИЗАЦИИ БЕЗОПАСНОСТИ ИНФОРМАЦИИ, СВЯЗАННОЙ С ФИЗИЧЕСКОЙ ЯДЕРНОЙ БЕЗОПАСНОСТЬЮ

Категория		Область	Чувствительность	Обоснование обеспечения безопасности
1. ФИЗИЧЕСКАЯ БЕЗОПАСНОСТЬ МАТЕРИАЛОВ И УСТАНОВОК				
1.1.	Регулирующие положения и руководящие материалы			
	A. Национальные регулирующие положения по национальной безопасности, регламентирующие использование ядерного материала или другого радиоактивного материала	N, R	Не чувствительная	Такая информация обычно публикуется в открытом доступе.
	B. Руководящие материалы по таким регулирующим положениям, изданные компетентным органом или другим государственным учреждением	N, R	Чувствительная	Хотя не все такие руководящие материалы могут быть чувствительными, документ такого рода может содержать подробную информацию о стандартах, типах оборудования, которое будет использоваться, процедурах и операциях по обеспечению национальной безопасности на установке. Такая подробная информация может быть полезна нарушителям, планирующим злоумышленное действие.
1.2.	Направления государственной политики в области физической ядерной безопасности			
	A. Общие направления государственной политики в отношении ядерного материала или другого радиоактивного материала	N, R	Не чувствительная	Такая информация обычно находится в открытом доступе.

ТАБЛИЦА II–1. УСЛОВНАЯ СХЕМА КАТЕГОРИЗАЦИИ БЕЗОПАСНОСТИ ИНФОРМАЦИИ, СВЯЗАННОЙ С ФИЗИЧЕСКОЙ ЯДЕРНОЙ БЕЗОПАСНОСТЬЮ (продолж.)

Категория		Область	Чувствительность	Обоснование обеспечения безопасности
	B. Подробная политика, охватывающая конкретные вопросы физической безопасности.	N, R	Чувствительная	Она может указывать на препятствия, с которыми могут столкнуться нарушители, позволяя им планировать получение более подробной информации.
1.3.	План обеспечения физической безопасности установки	N, R	Чувствительная	Обычно он содержит подробное описание мер физической безопасности, принятых на установке, и точную информацию о том, где на установки хранятся материалы. В случае ядерных установок планы также содержат подробную информацию о других областях, важных для эксплуатации площадки.
1.4.	Отчеты о физической безопасности			
	A. Отчеты об обследованиях, инспекциях и оценках в целях обеспечения физической безопасности и другие отчеты о мерах физической защиты или технических мерах физической безопасности, применяемых на площадке или установке	N, R	Чувствительная	Доступ к этим отчетам может предоставить злоумышленникам подробную информацию о местонахождении материала, мерах, принятых для его защиты, и любых оцененных уязвимостях, что может помочь им избежать воздействия мер физической безопасности и контроля.
	B. Отчеты, в которых описаны критические особенности и/или подчеркнуты требования по улучшению физической безопасности, в том числе в особо важных зонах (если применимо)	N, R	Чувствительная	Информация такого рода может быть полезна для нарушителей, желающих избежать воздействия мер физической безопасности, и может помочь в выборе установки в качестве цели.

ТАБЛИЦА II–1. УСЛОВНАЯ СХЕМА КАТЕГОРИЗАЦИИ БЕЗОПАСНОСТИ ИНФОРМАЦИИ, СВЯЗАННОЙ С ФИЗИЧЕСКОЙ ЯДЕРНОЙ БЕЗОПАСНОСТЬЮ (продолж.)

Категория		Область	Чувствительность	Обоснование обеспечения безопасности
C.	Результаты расследований физической безопасности на площадке или установке, в том числе в отношении утечек и потерь чувствительной информации	N, R	Чувствительная	Информация такого рода может быть полезна для нарушителей, желающих избежать воздействия мер физической безопасности, и может помочь в выборе установки в качестве цели.
D.	Отчеты с описанием уязвимостей системы менеджмента физической безопасности и последствий отказов	N, R	Чувствительная	Информация такого рода может быть полезна нарушителям, желающим обойти меры физической безопасности.
1.5.	Подробная информация о конструкции			
A.	Подробная информация о конструкции и о расположении мест, в которых может храниться или обрабатываться материал, включая чертежи или планы, хранящиеся на любых носителях, с указанием элементов физической защиты, имеющих отношение к предотвращению злоумышленных действий нарушителей	N, R	Чувствительная	Официальные карты, схемы или планы площадок могут быть опубликованы по усмотрению руководства площадки при условии, что они не содержат подробного описания аспектов зданий, материалов, хранящихся в зданиях, а также расположения внутренних защитных ограждений и других мер физической безопасности, применяемых в зданиях.
B.	Подробная информация о конструкции особо важных зон на атомных электростанциях и других ядерных установках	N	Чувствительная	Информация такого рода может быть полезна нарушителям, желающим избежать воздействия мер физической безопасности и может быть использована для целей саботажа (диверсии).

ТАБЛИЦА II–1. УСЛОВНАЯ СХЕМА КАТЕГОРИЗАЦИИ БЕЗОПАСНОСТИ ИНФОРМАЦИИ, СВЯЗАННОЙ С ФИЗИЧЕСКОЙ ЯДЕРНОЙ БЕЗОПАСНОСТЬЮ (продолж.)

Категория		Область	Чувствительность	Обоснование обеспечения безопасности
1.6.	Системы защиты			
	A. Подробная информация о любых используемых мерах физической защиты, например, тревожной сигнализации, камерах наблюдения, контроле доступа, персонале службы безопасности и т.д.	N, R	Чувствительная	Любая подробная информация такого рода будет полезна любому нарушителю, который пожелает нейтрализовать системы физической безопасности на установке.
	B. Типы и расположение датчиков системы обнаружения несанкционированного проникновения и связанных с ней камер наблюдения, включая их электрические принципиальные схемы, расположение критически важных источников питания, прокладки кабелей, программы технического обслуживания и тестирования этого оборудования	N, R	Чувствительная	
1.7.	Подробная информация об автоматизированных системах контроля доступа, включая расположение компьютерных серверов и резервных серверов и их источников питания	N, R	Чувствительная	Любую подробную информацию, которая может привести к тому, что система контроля доступа будет нейтрализована нарушителем, внешним или внутренним, не следует разглашать.

ТАБЛИЦА II–1. УСЛОВНАЯ СХЕМА КАТЕГОРИЗАЦИИ БЕЗОПАСНОСТИ ИНФОРМАЦИИ, СВЯЗАННОЙ С ФИЗИЧЕСКОЙ ЯДЕРНОЙ БЕЗОПАСНОСТЬЮ (продолж.)

Категория		Область	Чувствительность	Обоснование обеспечения безопасности
1.8.	Хранилища: процедуры обеспечения физической безопасности при выдаче, получении и контроле материала в хранилище; фамилии уполномоченных обладателей ключей; меры мониторинга и охраны	N, R	Чувствительная	Информация потенциально полезна для нарушителей, планирующих злоумышленные действия.
1.9.	Общие карты, показывающие положение и границы установки, но без подробной информации о том, что находится внутри	N, R	Не чувствительная	Свободно доступные картографические приложения в Интернете четко отображают такую информацию.
1.10.	Другие вопросы, связанные с физической защитой, например, местонахождение, компоновка, численность персонала и оборудование центрального пункта тревожной сигнализации; расположение вторичного пункта тревожной сигнализации; тип барьера внутренней зоны	N, R	Чувствительная	Любая подробная информация такого рода была бы весьма полезна любому нарушителю, желающему нейтрализовать системы физической безопасности на ядерных установках.
	2. ИНФОРМАЦИЯ О КОЛИЧЕСТВЕ И ФОРМЕ МАТЕРИАЛА			
2.1.	Информация о количестве, типе и форме ядерного материала, включая источники, полученные или хранящиеся в определенных местах на всех категориях площадок и атомных электростанций, включая точные места хранения отработавшего топлива	N	Чувствительная	Этот тип информации может быть полезен нарушителям, выбирающим цели при планировании нападений.

ТАБЛИЦА II–1. УСЛОВНАЯ СХЕМА КАТЕГОРИЗАЦИИ БЕЗОПАСНОСТИ ИНФОРМАЦИИ, СВЯЗАННОЙ С ФИЗИЧЕСКОЙ ЯДЕРНОЙ БЕЗОПАСНОСТЬЮ (продолж.)

Категория		Область	Чувствительность	Обоснование обеспечения безопасности
2.2.	Пропускная способность — номинальная производительность, фактическая пропускная способность и исторические данные о пропускной способности установки, находящейся под гарантиями МАГАТЭ	N	Не чувствительная	Такая информация высокого уровня, особенно для атомных электростанций, часто находится в открытом доступе.
2.3.	Инвентарные количества, национальные или местные, другого радиоактивного материала (включая изъятый из употребления материал), включая количество, тип, форму и точное местонахождение	R	Чувствительная	Этот тип информации может быть полезен нарушителям, выбирающим цели при планировании нападений с целью хищения радиоактивного материала. Следует учитывать, какая информация уже является общедоступной в отношении таких инвентарных количеств. Вся такая информация не может считаться конфиденциальной. Процессы, основанные на учете рисков, помогут определить, следует ли обозначать что-либо как чувствительное.
	3. МАТЕРИАЛ В ПРОЦЕССЕ ПЕРЕВОЗКИ (ВКЛЮЧАЯ ПЕРЕМЕЩЕНИЕ В ПРЕДЕЛАХ ПЛОЩАДКИ)			
3.1.	Информация о перемещениях ядерного материала категорий I, II, III	N	Чувствительная	Такая информация могла бы помочь в выборе целей при планировании злоумышленных действий, связанных с ядерным материалом в процессе перевозки.
3.2.	Транспортные средства повышенной безопасности (ТСПБ)			

ТАБЛИЦА II–1. УСЛОВНАЯ СХЕМА КАТЕГОРИЗАЦИИ БЕЗОПАСНОСТИ ИНФОРМАЦИИ, СВЯЗАННОЙ С ФИЗИЧЕСКОЙ ЯДЕРНОЙ БЕЗОПАСНОСТЬЮ (продолж.)

Категория		Область	Чувствительность	Обоснование обеспечения безопасности
A.	Визуальный доступ к внутренней части кабины и грузового отсека	N	Чувствительная	ТСПБ – это транспортные средства, специально разработанные для безопасной перевозки ядерного материал. ТСПБ перевозят ядерный материал, и любой тип информации, перечисленный в этом разделе, может быть полезен нарушителю, планирующему попытку хищения или саботажа (диверсии) в отношении ядерного материала в процессе перевозки.
B.	Особенности физической защиты при проектировании и создании транспортного средства	N	Чувствительная	
C.	Конструкция и функции сигнализаций, устройств иммобилизации и конструкции ключей для специальных замков	N	Чувствительная	
D.	Ключи от грузового отсека, запасные ключи и комбинации цифр кодовых замков, если они использовались	N	Чувствительная	
E.	Система слежения за транспортными средствами, если она установлена на ТСПБ; производительность и связь системы	N	Чувствительная	
3.3.	Контейнеры для перевозки ядерного материала			
A.	Уровень устойчивости транспортных контейнеров к нападениям различного рода	N	Чувствительная	Полезно для нарушителя, планирующего диверсионное нападение с целью высвобождения ядерного материала или планирующего хищение материала во время перевозки.
B.	Спецификации и данные о конструкции контейнеров	N	Не чувствительная	Информация о конструкции таких контейнеров без указания подробных сведений о конструкции часто доступна в Интернете.

ТАБЛИЦА II–1. УСЛОВНАЯ СХЕМА КАТЕГОРИЗАЦИИ БЕЗОПАСНОСТИ ИНФОРМАЦИИ, СВЯЗАННОЙ С ФИЗИЧЕСКОЙ ЯДЕРНОЙ БЕЗОПАСНОСТЬЮ (продолж.)

Категория		Область	Чувствительность	Обоснование обеспечения безопасности
	C. Информация о конструкции конкретных контейнеров (особо защищенных контейнеров)	N	Чувствительная	Полезна для нарушителя, планирующего диверсионное нападение с целью высвобождения ядерного материала или планирующего хищение материала во время перевозки.
3.4.	Транспортные упаковки: информация о конструкции транспортных упаковок	N	Чувствительная	Полезна для нарушителя, планирующего диверсионное нападение с целью высвобождения ядерного материала или планирующего хищение материала во время перевозки.
3.5.	Информация о перемещениях другого радиоактивного материала	R	Чувствительная	Этот тип информации, особенно если речь идет о перевозке мощных источников излучения, может быть полезен при планировании хищения.
	4. ИТ-СИСТЕМЫ И КОМПЬЮТЕРНЫЕ СИСТЕМЫ, ВАЖНЫЕ ДЛЯ ФИЗИЧЕСКОЙ БЕЗОПАСНОСТИ И БЕЗОПАСНОСТИ			
4.1.	Подробная информация об ИТ-системах, хранящих и обрабатывающих чувствительную информацию, включая системы, используемые в целях обеспечения физической безопасности, архитектуре системы, подробная информация об используемых мерах компьютерной безопасности и местонахождении резервных носителей информации	N, R	Чувствительная	Информация, полезная для нарушителя, планирующего злоумышленное действие на установке.

ТАБЛИЦА II–1. УСЛОВНАЯ СХЕМА КАТЕГОРИЗАЦИИ БЕЗОПАСНОСТИ ИНФОРМАЦИИ, СВЯЗАННОЙ С ФИЗИЧЕСКОЙ ЯДЕРНОЙ БЕЗОПАСНОСТЬЮ (продолж.)

Категория		Область	Чувствительность	Обоснование обеспечения безопасности
4.2.	Подробная информация о контроле доступа, системах обнаружения несанкционированного проникновения, системах мониторинга тревожной сигнализации, системах оценки и видеонаблюдения и других функциях и устройствах физической безопасности; и информация о местонахождении резервного оборудования и программного обеспечения	N, R	Чувствительная	Информация, полезная для нарушителя, планирующего злоумышленное действие на установке.
4.3.	Подробная информация о связанных с безопасностью ИТ-системах или компьютерных системах, важных для обеспечения безопасности, включая сведения о местах расположения, функциях, способах обновления, электропитании и резервном копировании	N, R	Чувствительная	Такие системы имеют функции управления и технологического мониторинга. Успешный взлом этих систем может позволить нарушителю как минимум нарушить работу установки, а в худшем случае нарушение может привести к радиоактивному выбросу.
	5. СИЛЫ ОХРАНЫ И СИЛЫ РЕАГИРОВАНИЯ			
5.1.	Силы охраны на установке			
	A. Общий состав и имеющиеся возможности сил	N	Не чувствительная	Предание гласности информации о существовании сил может успокоить общественность и потенциально действовать как сдерживающий фактор.

ТАБЛИЦА II–1. УСЛОВНАЯ СХЕМА КАТЕГОРИЗАЦИИ БЕЗОПАСНОСТИ ИНФОРМАЦИИ, СВЯЗАННОЙ С ФИЗИЧЕСКОЙ ЯДЕРНОЙ БЕЗОПАСНОСТЬЮ (продолж.)

Категория		Область	Чувствительность	Обоснование обеспечения безопасности
B.	Состав и имеющиеся возможности на конкретных установках	N	Чувствительная	Информация такого рода может быть полезна любому нарушителю при планировании проникновения на площадку ядерной установки с целью саботажа (диверсии) или хищения и может подорвать возможности эффективного реагирования на нападение.
C.	Количества персонала в любой смене на площадке	N	Чувствительная	
D.	Оружие и другое специальное снаряжение, имеющееся в распоряжении сил охраны, и количество сотрудников в частях сил охраны на конкретных площадках, обученных пользованию огнестрельным оружием	N	Чувствительная	Любую информацию, которая может помочь нарушителю заранее оценить масштабы реагирования и возможности, имеющиеся в тактическом оперативном подразделении, следует защищать от разглашения.
E.	Местонахождение сил реагирования, их возможности, вооружение, транспортные средства специального назначения и сроки реагирования на площадке	N	Чувствительная	
F.	Планы развертывания	N	Чувствительная	
5.2.	Сопровождение при перемещениях ядерного материала			

ТАБЛИЦА II–1. УСЛОВНАЯ СХЕМА КАТЕГОРИЗАЦИИ БЕЗОПАСНОСТИ ИНФОРМАЦИИ, СВЯЗАННОЙ С ФИЗИЧЕСКОЙ ЯДЕРНОЙ БЕЗОПАСНОСТЬЮ (продолж.)

Категория		Область	Чувствительность	Обоснование обеспечения безопасности
A.	Развертывание и возможности службы сопровождения	N	Чувствительная	Информация может быть полезна нарушителю, планирующему нападение на конвой.
B.	Используемые радиочастоты для обеспечения связи с силами реагирования или местной полицией	N	Чувствительная	
	6. УЧЕТ ЯДЕРНОГО МАТЕРИАЛА			
6.1.	Описание			
A.	Изложение общих принципов учета материала	N	Не чувствительная	Сведения об общих принципах такого рода имеются в открытом доступе.
B.	Вопросник и описание информации о конструкции, а также расположение зон баланса материала (ЗБМ) и ключевых точек измерения (КТИ)	N	Чувствительная	Такая подробная информация о местонахождении и количестве ядерного материала может быть полезна нарушителю, планирующему злоумышленное действие.
C.	Физическая и химическая форма измерения материала в КТИ	N	Чувствительная	
6.2.	Данные измерений и контрольно-измерительных приборов			
A.	Прецизионность и точность стандартных лабораторных методов	N	Не чувствительная	Эта информация часто находится в открытом доступе.

ТАБЛИЦА II–1. УСЛОВНАЯ СХЕМА КАТЕГОРИЗАЦИИ БЕЗОПАСНОСТИ ИНФОРМАЦИИ, СВЯЗАННОЙ С ФИЗИЧЕСКОЙ ЯДЕРНОЙ БЕЗОПАСНОСТЬЮ (продолж.)

Категория		Область	Чувствительность	Обоснование обеспечения безопасности
	B. Данные, которые показывают чувствительность измерения или пороги срабатывания сигнализации для количества неучтенного материала (КНМ) на конкретной станции	N	Чувствительная	Совокупные или отдельные данные о прецизионности и точности, относящиеся к фактическим или типичным измерениям на площадках, могут быть полезны нарушителю, планирующему хищение материала.
6.3.	Данные о потоках и инвентарных количествах ядерного материала, хранящиеся в ИТ-системах, в печатном виде или на любом носителе данных	N	Чувствительная	Информация может раскрыть точную информацию о местонахождении и перемещениях ядерного материала.
6.4.	Количество неучтенного материала			
	A. Годовые показатели КНМ для площадки, которые не раскрывают соответствующую ЗБМ	N	Не чувствительная	Во многих государствах совокупные годовые показатели КНМ публикуются или могут публиковаться в открытом доступе.
	B. КНМ в ЗБМ или КТИ	N	Чувствительная	
	C. Подробная информация о расследованиях в отношении конкретного КНМ, если официально не разрешено раскрытие информации.	N	Чувствительная	Однако подробная информация о КНМ или результаты расследования могут быть полезны нарушителю при планировании нападения на конкретную установку и поэтому их следует считать чувствительными.
	D. Предел погрешности для КНМ или другие конкретные указания на неопределенность информации о значениях КНМ.	N	Чувствительная[a]	

[a] В некоторых государствах предел погрешности для КНМ не считается чувствительной информацией.

ТАБЛИЦА II–1. УСЛОВНАЯ СХЕМА КАТЕГОРИЗАЦИИ БЕЗОПАСНОСТИ ИНФОРМАЦИИ, СВЯЗАННОЙ С ФИЗИЧЕСКОЙ ЯДЕРНОЙ БЕЗОПАСНОСТЬЮ (продолж.)

Категория		Область	Чувствительность	Обоснование обеспечения безопасности
7. ЗАЯВКИ В РАМКАХ ПРОЦЕССА ЛИЦЕНЗИРОВАНИЯ И ВЫДАЧИ РАЗРЕШЕНИЙ				
7.1.	Заявки в рамках процесса лицензирования и выдачи разрешений без подробной информации о мерах физической безопасности; типе, форме и количестве материала	N, R	Не чувствительная	Содержание такой заявки будет варьироваться в зависимости от регулирующей основы и конкретного конечного использования. Если заявки содержат чувствительную информацию, которая потенциально может быть использована нарушителем, то такую заявку также следует рассматривать как чувствительную информацию.
7.2.	Заявки в рамках процесса лицензирования и выдачи разрешений , содержащие подробную информацию, например, о мерах физической безопасности, а также о типе, форме и количестве материала	N, R	Чувствительная	Содержание такой заявки будет варьироваться в зависимости от регулирующей основы и конкретного конечного использования. Если заявки содержат чувствительную информацию, которая потенциально может быть использована нарушителем, то такую заявку также следует рассматривать как чувствительную информацию.

ТАБЛИЦА II–1. УСЛОВНАЯ СХЕМА КАТЕГОРИЗАЦИИ БЕЗОПАСНОСТИ ИНФОРМАЦИИ, СВЯЗАННОЙ С ФИЗИЧЕСКОЙ ЯДЕРНОЙ БЕЗОПАСНОСТЬЮ (продолж.)

Категория		Область	Чувствительность	Обоснование обеспечения безопасности
	8. ОБОСНОВАНИЯ ПО БЕЗОПАСНОСТИ, ТЕХНИЧЕСКАЯ ДОКУМЕНТАЦИЯ И ДРУГАЯ ИНФОРМАЦИЯ ПО БЕЗОПАСНОСТИ ИЛИ ЭКОЛОГИИ			
8.1.	Обоснования безопасности всех классов			Хотя большая часть информации, касающейся обоснований безопасности, может быть опубликована для обеспечения прозрачности, некоторая информация может считаться чувствительной в отношении физической ядерной безопасности.
A.	Подробная информация о потенциальных опасностях или другая информация, которая может быть использована для оценки воздействия выброса, или подробная информация о воздействиях выбросов	N, R	Чувствительная	Такая подробная информация, содержащаяся в обоснованиях безопасности, может быть полезна нарушителю для выбора целей и планирования операции.
B.	Подробная информация о сильных и слабых сторонах процессов, структур, и систем защиты, спроектированных с целью локализации, контроля или обеспечения сохранности ядерного материала или другого радиоактивного материала	N, R	Чувствительная	

ТАБЛИЦА II–1. УСЛОВНАЯ СХЕМА КАТЕГОРИЗАЦИИ БЕЗОПАСНОСТИ ИНФОРМАЦИИ, СВЯЗАННОЙ С ФИЗИЧЕСКОЙ ЯДЕРНОЙ БЕЗОПАСНОСТЬЮ (продолж.)

Категория		Область	Чувствительность	Обоснование обеспечения безопасности
C.	Подробная информация о доступе к производственному технологическому процессу, как о физическом контроле доступа, так и об изъятии материала из технологического процесса в целях контроля и мониторинга	N, R	Чувствительная	
	9. ПЛАНЫ ЧРЕЗВЫЧАЙНЫХ МЕР И РЕАГИРОВАНИЯ И СООТВЕТСТВУЮЩИЕ УЧЕНИЯ			
9.1.	Чрезвычайные меры и реагирование			
A.	Наличие плана чрезвычайных мер и реагирования	N, R	Не чувствительная	Огласка существования планов может успокоить общественность и потенциально действовать как сдерживающий фактор.
B.	Подробное содержание плана чрезвычайных мер и реагирования	N, R	Чувствительная	Детали плана могут указывать на возможности, ограничения и время реагирования и, следовательно, быть полезными нарушителю при планировании преднамеренного нападения.
9.2.	Планы чрезвычайных мер по обеспечению физической безопасности, включая подробную информацию	N, R	Чувствительная	Такие документы содержат информацию о существующих мерах физической безопасности, о возможностях отдельных групп полиции или сил охраны и о вероятном реагировании на инцидент, связанный с физической безопасностью.

ТАБЛИЦА II–1. УСЛОВНАЯ СХЕМА КАТЕГОРИЗАЦИИ БЕЗОПАСНОСТИ ИНФОРМАЦИИ, СВЯЗАННОЙ С ФИЗИЧЕСКОЙ ЯДЕРНОЙ БЕЗОПАСНОСТЬЮ (продолж.)

Категория		Область	Чувствительность	Обоснование обеспечения безопасности
9.3.	Учения			
	A. Учения должны быть проведены или уже проводились	N, R	Не чувствительная	Публикация информации о проведении учений может успокоить общественность при условии, что уровень детализации не поможет нарушителю узнать например, дату/время/место проведения будущих учений.
	B. Подробная информация об учениях по обеспечению физической безопасности на площадке, включая сценарий, какие аспекты плана обеспечения физической безопасности проверяются, будут ли задействованы силы реагирования, а также результаты учений	N, R	Чувствительная	Предоставляет нарушителям информацию о характере, численности, возможностях и времени реагирования служб реагирования, подробные сведения о вооруженных силах реагирования, характере применяемой тактики и схеме связи.
	C. Подробная информация об учениях по обеспечению безопасности	N, R	Не чувствительная	Учения по обеспечению безопасности часто проводятся открыто и прозрачно. Обычно сведения можно считать нечувствительными, если они не раскрывают подробную информацию о мерах физической безопасности.

ТАБЛИЦА II–1. УСЛОВНАЯ СХЕМА КАТЕГОРИЗАЦИИ БЕЗОПАСНОСТИ ИНФОРМАЦИИ, СВЯЗАННОЙ С ФИЗИЧЕСКОЙ ЯДЕРНОЙ БЕЗОПАСНОСТЬЮ (продолж.)

Категория		Область	Чувствительность	Обоснование обеспечения безопасности
	10. ПЕРСОНАЛЬНАЯ ИНФОРМАЦИЯ			
10.1	Персональная информация			
	A. Информация, полученная в результате проверки благонадежности	N, R	Чувствительная	Информация такого характера может быть использована для шантажа или вымогательства. Большинство национальных регулирующих положений о частной жизни предписывают защиту информации этого типа.
	B. Информация в личных делах	N, R	Чувствительная	
	11. ИНВЕНТАРНЫЕ КОЛИЧЕСТВА РАДИОАКТИВНЫХ ОТХОДОВ			
11.1	Информация о радиоактивных отходах			
	A. Общая информация о запасах, не содержащая никакой информации, которую можно было бы использовать, например, тот факт, что отходы хранятся на определенной площадке, или сведения о совокупном количестве отходов без указания их местонахождения	N	Не чувствительная	Такая информация, как правило, находится в открытом доступе и не описывает особенности использования, полезные для нарушителя.
	B. Информация, которая может быть использована в злоумышленном действии или позволяет идентифицировать конкретное здание на установке и хранящийся там материал	N	Чувствительная	Такая информация содержит сведения о цели для нарушителя, планирующего саботаж (диверсию).

ТАБЛИЦА II–1. УСЛОВНАЯ СХЕМА КАТЕГОРИЗАЦИИ БЕЗОПАСНОСТИ ИНФОРМАЦИИ, СВЯЗАННОЙ С ФИЗИЧЕСКОЙ ЯДЕРНОЙ БЕЗОПАСНОСТЬЮ (продолж.)

Категория		Область	Чувствительность	Обоснование обеспечения безопасности
	12. ВЫВОД ИЗ ЭКСПЛУАТАЦИИ			
12.1	Планы по выводу станции из эксплуатации	N, R	Не чувствительная	Планы по выводу установок из эксплуатации часто объявляются публично.
12.2	Отходы при выводе из эксплуатации[b]			
	A. Сведения о планах сооружения хранилища и о его местонахождении.	N, R	Не чувствительная	Эта информация часто находится в открытом доступе.
	B. Подробная информация о конструкции, мерах физической безопасности и количестве или типе материала, который должен храниться в новых зданиях для обработки и хранения отходов и загрязненного материала, образующегося в результате деятельности по переработке во время вывода из эксплуатации	N, R	Чувствительная	Эта информация может содержать полезные сведения для нарушителя, планирующего диверсионные нападения.

[b] Это относится главным образом к загрязненным материалам с установки, а не к радиоактивным отходам технологических процессов, осуществляемых при нормальной эксплуатации установки.

ТАБЛИЦА II–1. УСЛОВНАЯ СХЕМА КАТЕГОРИЗАЦИИ БЕЗОПАСНОСТИ ИНФОРМАЦИИ, СВЯЗАННОЙ С ФИЗИЧЕСКОЙ ЯДЕРНОЙ БЕЗОПАСНОСТЬЮ (продолж.)

Категория		Область	Чувствительность	Обоснование обеспечения безопасности
13. ОЦЕНКА УГРОЗ И ИНФОРМАЦИЯ ДЛЯ ОПОВЕЩЕНИЯ ОБ УГРОЗАХ ФИЗИЧЕСКО БЕЗОПАСНОСТИ				
13.1.	Оценки угроз, выпущенные государством, органами национальной безопасности или другими компетентными органами	N, R	Чувствительная	Обычно составляются на основе материалов по национальной безопасности, например, информации от национальных разведывательных служб.
13.2	Подробная информация о проектной угрозе	N	Чувствительная	Обычно составляется на основе материалов по национальной безопасности, например, информации от национальных разведывательных служб.
13.3.	Подробная информация об исследовании по идентификации особо важных зон	N	Чувствительная	Может быть полезна нарушителю при определении целей и проведении нападения.
13.4	Причины любого существующего состояния оповещения об угрозах физической безопасности и любых его изменений	N, R	Чувствительная	Обычно определяются на основе материалов по национальной безопасности, например, информации от национальных разведывательных служб.
14. ЯДЕРНАЯ ТЕХНОЛОГИЯ				
14.1.	Подробная техническая информация о производстве или переработке ядерного материала (например, обработка и переработка обогащенного урана)	N	Чувствительная	Информация такого типа может быть полезна нарушителю.

ТАБЛИЦА II–1. УСЛОВНАЯ СХЕМА КАТЕГОРИЗАЦИИ БЕЗОПАСНОСТИ ИНФОРМАЦИИ, СВЯЗАННОЙ С ФИЗИЧЕСКОЙ ЯДЕРНОЙ БЕЗОПАСНОСТЬЮ (продолж.)

Категория		Область	Чувствительность	Обоснование обеспечения безопасности
14.2	Конструкции или новые технологии, представленные для лицензирования (например, технология усовершенствованных реакторов и т. д.)	N	Чувствительная	Хотя подробная информация об этих технологиях может доводиться до сведения общественности, возможно, что некоторые детали конструкции или технологии могут быть использованы нарушителями для целей планирования. Такая информация может быть проверена на наличие чувствительной информации.
14.3.	Подробная информация, которая поможет раскодировать устройства для получения доступа к источникам или иным образом поможет обойти меры безопасности	R	Чувствительная	Эта информация может быть полезна нарушителю, пытающемуся удалить радиоактивный материал.
14.4.	Исследования уязвимостей технологических разработок	N, R	Чувствительная	Хотя академические исследования могут быть общедоступными, любую подробную информацию, раскрывающую уязвимости, которые могут быть использованы нарушителем, следует защищать от несанкционированного раскрытия.

ТАБЛИЦА II–1. УСЛОВНАЯ СХЕМА КАТЕГОРИЗАЦИИ БЕЗОПАСНОСТИ ИНФОРМАЦИИ, СВЯЗАННОЙ С ФИЗИЧЕСКОЙ ЯДЕРНОЙ БЕЗОПАСНОСТЬЮ (продолж.)

Категория	Область	Чувствительность	Обоснование обеспечения безопасности
15. ИСТОРИЧЕСКАЯ ИНФОРМАЦИЯ			
15.1. Историческая информация, актуальная в настоящее время и все еще чувствительная, независимо от того, является ли эта информация секретной	N, R	Чувствительная	Информация такого рода, хотя она и старая, все еще может быть полезной для нарушителей.

Примечание: ТСПБ — транспортное средство повышенной безопасности; КТИ — ключевая точка измерения; ЗБМ — зона баланса материала; КНМ — количество неучтенного материала; N — ядерный материал и ядерные установки; R — другой радиоактивный материал и связанные с ним установки.

Приложение III

ОБРАЗЕЦ ПРОГРАММЫ ПОВЫШЕНИЯ ОСВЕДОМЛЕННОСТИ О ФИЗИЧЕСКОЙ БЕЗОПАСНОСТИ

III–1. В Приложении III представлены примерная структура и содержание программы повышения осведомленности о физической безопасности. При принятии решения о содержании программы повышения осведомленности об информационной безопасности начальнику службы безопасности организации следует учитывать конкретную актуальность выделенных здесь тем и методов и соответствующим образом адаптировать эту программу.

ОБУЧЕНИЕ В ОБЛАСТИ ФИЗИЧЕСКОЙ БЕЗОПАСНОСТИ

III–2. Обучение можно в целом разделить на четыре типа:

a) вводный курс улучшает осведомленность об угрозах и уязвимостях и признание необходимости защиты данных, информации и средств их обработки (осведомленность о компьютерной и информационной безопасности);
b) тематическое обучение включает курсы по конкретным аспектам физической безопасности для всего персонала (работа с засекреченными материалами и процедуры информационной безопасности);
c) профессиональное обучение, как правило, представляет собой детальное техническое обучение персонала, имеющего конкретные должностные обязанности, например, наряду с прочими, системных администраторов, разработчиков программного обеспечения, сетевых администраторов, охранников, специалистов по засекречиванию и рассекречиванию документов;
d) специализированное обучение по вопросам физической безопасности, направленное на обучение на уровне экспертов и проводимое обычно для руководителей, в таких областях, как управление рисками, предотвращение инцидентов и реагирование на них.

III–3. Программа может включать материалы с целью повышения осведомленности по следующим темам:

a) обзор национальной инфраструктуры физической безопасности;

b) аспекты информационной безопасности и почему они важны для физической ядерной безопасности;
c) национальная система классификации;
d) принципы обеспечения физической безопасности, например, «необходимо знать» и «необходимо сохранять»;
e) современные угрозы физической безопасности, возникающие в результате следующих преднамеренных действий:
    i) враждебных разведывательных служб в отношении шпионажа и передачи технологий;
    ii) подрывных организаций;
    iii) других лиц и групп, такие как информационные посредники и журналисты-расследователи, стремящихся получить несанкционированный доступ к чувствительной информации или ядерным площадкам и установкам;
    iv) внутренних нарушителей;
f) угроза со стороны вражеских организаций и угроза диверсий с учетом современной мировой угрозы со стороны любых экстремистских группировок;
g) риски и последствия внутренней утраты или утечек чувствительной информации, возможно, в результате непреднамеренного поведения или с целью создания затруднений, а также преднамеренного предательства по политическим мотивам или для оказания помощи терроризму;
h) поведение или действия, способные оказать помощь потенциальным нарушителям или увеличить риск раскрытия информации, в том числе:
    i) беспечное поведение, такое как небрежное отношение к физической безопасности и безответственные заявления;
    ii) непреднамеренное поведение, которое может привлечь внимание враждебных служб, и меры предосторожности, необходимые в повседневной деятельности, включая, например, социальные подходы, путешествия, переписку и знакомства;
i) информация о актуальных событиях в области физической безопасности или новых подходах, используемых враждебными учреждениями, которую следует быстро распространять;
j) подчеркивание необходимости немедленно сообщать обо всех подозрительных обстоятельствах, предполагаемых недостатках в процедурах обеспечения физической безопасности или беспечном поведении, проявляющемся у коллег — следует быть полностью информированным о том, как это незаметно используется;

k) действие национальных законов и правил и их актуальность для отдельных лиц, например, законов, регулирующие тайну, борьбу с терроризмом, безопасность, защиту данных и свободу информации, а также санкции и наказание за нарушение;

l) объяснение уровней допуска к секретным материалам; как осуществляются проверки благонадежности; зачем они нужны в атомной и радиологической отраслях; и какие уровни доступа связаны с конкретными уровнями допуска и благонадежности и, кроме того, как это связано с угрозами физической безопасности, упомянутыми выше;

m) отказ в обслуживании (например, предотвращение доступа организации к информации, когда это необходимо, включая такие действия, как хищение) или уничтожение — нарушение доступности;

n) несанкционированное изменение информации или вмешательство в информацию — нарушение ее целостности;

o) несанкционированное раскрытие информации — нарушение конфиденциальности.

III–4. Программа может включать материалы для обучения участников по следующим темам:

a) безопасность информации о ядерном материале и другом радиоактивном материале и установках;

b) надлежащая практика и процедуры обеспечения физической безопасности, включая:
   i) правильное использование классов чувствительности информации;
   ii) физическую защиту, безопасность персонала и информационную безопасность (например, документов, средств связи и компьютеров);
   iii) практические примеры применения правил и процедур физической безопасности в задачах, которые сотрудники выполняют или будут выполнять;
   iv) действия, которые должны быть предприняты в случае подозрения в нарушении или обнаружения нарушения физической безопасности.

ДОПОЛНИТЕЛЬНЫЕ СПОСОБЫ СОДЕЙСТВИЯ ОБЕСПЕЧЕНИЮ ФИЗИЧЕСКОЙ БЕЗОПАСНОСТИ

III–5. В дополнение к базовой программе обучения существует ряд других методов, с помощью которых информационные сообщения о физической безопасности могут быть доведены до сведения сотрудников и подрядчиков:

a) регулярные информационные бюллетени по вопросам физической безопасности, публикуемые органами национальной безопасности. В них могут быть изложены вопросы, представляющие актуальный интерес, и рекомендации по целому ряду вопросов физической безопасности;
b) плакаты, напоминающие об угрозах физической безопасности и об основных мерах контроля физической безопасности, необходимых для противодействия им. Их эффективность имеет тенденцию быть временной, поэтому плакаты следует не только размещать на видных местах, но и часто менять;
c) наклейки, напоминающие сотрудникам об их личной ответственности за обеспечение физической безопасности при использовании конкретных элементов оборудования;
d) уведомления о необходимости соблюдении безопасности на этапе запуска (загрузки) компьютерной системы, ознакомление с которыми пользователь должен подтвердить, прежде чем компьютер завершит загрузку или вход в систему. (Системы могут регистрировать такие подтверждения, с тем чтобы пользователь не мог отрицать, что не видел уведомление);
e) уведомления по вопросам физической безопасности, бюллетени и циркуляры, составленные руководством службы безопасности с целью напоминания персоналу об определенных правилах физической безопасности, в том числе с целью противодействия возможной самоуспокоенности;
f) повышение осведомленности о случаях нарушений физической безопасности и уроках, которые необходимо извлечь из них;
g) предупреждение отдельных лиц о конкретных или актуальных угрозах физической безопасности и предоставление рекомендаций по противодействию им;
h) предоставление канала связи с отдельными лицами по вопросам физической безопасности в целом;
i) регулярные периодические проверки индивидуальных знаний в области физической безопасности;

j) сеть Интранет организации также может быть ценным инструментом для передачи или продвижения сообщения о физической безопасности, если характер и конфиденциальность материала остаются в пределах аккредитованного уровня секретности для сети.

ГЛОССАРИЙ

доступность. Свойство быть доступным и пригодным для использования по требованию уполномоченного органа.

другой радиоактивный материал. Любой радиоактивный материал, не являющийся ядерным материалом.

информационная безопасность. Сохранение конфиденциальности, целостности и доступности информации.

информационный объект. Знания или данные, имеющие ценность для организации.

компетентный орган. Правительственная организация или учреждение, назначенное государством для выполнения одной или нескольких функций в области физической ядерной безопасности.

конфиденциальность. Свойство, заключающееся в том, что информация не предоставляется и не раскрывается неуполномоченным лицам, объектам или процессам.

«необходимо знать». Правило, согласно которому отдельным лицам, процессам и системам предоставляется доступ только к той информации, возможностям и активам, которые необходимы для выполнения их санкционированных функций.

«необходимо сохранять». Правило, согласно которому физическим лицам разрешается иметь в своем физическом владении только те информационные активы, которые необходимы для эффективного выполнения их работы.

радиоактивный материал. Любой радиоактивный материал, не являющийся ядерным материалом.

раскрытие. Случайное или преднамеренное нарушение конфиденциальности, утрата целостности или утрата доступности информационного объекта.

целостность. Свойство точности и полноты информации.

чувствительная информация. Информация в любой форме, включая программное обеспечение, несанкционированное раскрытие, корректировка, изменение, уничтожение или неиспользование которой может поставить под угрозу ядерную безопасность.

чувствительные информационные активы. Любое оборудование или компоненты, которые используются для хранения, обработки, управления или передачи чувствительной информации. Например, чувствительные информационные активы включают системы управления, сети, информационные системы и любые другие электронные или физические носители.

ядерный материал. Любой материал, который является либо специальным расщепляющимся материалом, либо исходным материалом, как он определен в статье XX Устава МАГАТЭ.

ЗАКАЗ В СТРАНАХ

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

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

СЕВЕРНАЯ АМЕРИКА

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

ОСТАЛЬНЫЕ СТРАНЫ

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

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

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

Индивидуальные заказы:
www.eurospanbookstore.com/iaea

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

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

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

МЕЖДУНАРОДНОЕ АГЕНТСТВО ПО АТОМНОЙ ЭНЕРГИИ
ВЕНА