60 лет
IAEA Атом для мира и развития

Генеральная конференция

GC(60)/INF/10
25 сентября 2016 года

Общее распространение
Русский
Язык оригинала: английский

Шестидесятая очередная сессия

Пункт 13 предварительной повестки дня
(GC(60)/1, Add.1, Add.2 и Add.3)

Сообщение Председателя Международной группы по ядерной безопасности (ИНСАГ) от 20 июля 2016 года

20 июля 2016 года Генеральный директор получил письмо Председателя ИНСАГ Ричарда Месерва, в котором представлены его соображения по нынешним новым вопросам безопасности. Настоящим вышеупомянутое письмо распространяется для сведения Генеральной конференции.

ИНСТИТУТ НАУКИ КАРНЕГИ

20 июля 2016 года

Уважаемый Генеральный директор Амано,

Обращаюсь к Вам в своем качестве Председателя Международной группы по ядерной безопасности (ИНСАГ). Как это предусмотрено ее кругом ведения, ИНСАГ готовит «рекомендации и высказывает мнения относительно нынешних новых проблем безопасности» для МАГАТЭ и других сторон. Находясь на посту Председателя, я традиционно стремился выполнять эту обязанность не только путем представления различных докладов ИНСАГ, но также посредством ежегодного письма. Мои предыдущие письма размещены на сайте ИНСАГ по адресу: http://goto.iaea.org/insag. Настоящее послание представляет собой письмо за этот год.

В предыдущих письмах я обычно заострял внимание на конкретных вопросах, представляющих интерес в данный момент времени. Например, в своем письме от 21 августа 2015 года я обратился к проблеме внешних природных событий и возникающих в связи с ними трудностей для систем безопасности. В этом году я намерен применить другой подход. Настоящее письмо посвящено стратегическому вопросу – необходимости учитывать недостатки институционального и культурного характера, которые могут стать коренными причинами ядерных аварий. В письме приводятся основные моменты готовящегося к публикации доклада ИНСАГ 2016 года по этой теме «Ensuring Robust National Nuclear Safety Systems- Institutional Strength in Depth» («Обеспечение надежности национальных систем ядерной безопасности. Глубокоэшелонированная институциональная защита») (INSAG-27) (в печати).

Как указано во всеобъемлющем докладе МАГАТЭ, после аварии на АЭС «Фукусима-дайити» необходимо определить и закрепить множество технических уроков. Кроме того, в этом докладе сделано одно замечание общего характера, которое является отправной точкой для дальнейшей работы ИНСАГ. В докладе отмечено: «Системный подход к безопасности должен учитывать взаимодействие между человеческими, организационными и техническими факторами». При несомненной необходимости строгих и комплексных норм безопасности и инструментов, позволяющих обеспечивать высокий уровень безопасности, крайне важно также наличие сети учреждений и каналов взаимодействия в рамках этих учреждений и между ними, обеспечивающее правильное и действенное применение этих инструментов. Мы называем такую схему «глубокоэшелонированной институциональной защитой» (ГэИЗ). ГэИЗ дополняет и расширяет концепцию глубокоэшелонированной защиты, которая играет главную роль при анализе уровней технических систем, предназначенных для предотвращения аварий на ядерных установках или смягчения их последствий (см. «Глубокоэшелонированная защита в ядерной безопасности» (Серия ИНСАГ, № 10, 1998 год)).

Г-ну Юкии Амано
Генеральному директору
МАГАТЭ

В основе концепции ГэИЗ лежат три независимые институциональные подсистемы, которые при правильном использовании работают на предупреждение ядерной аварии. Этими подсистемами являются: 1) мощная ядерная отрасль; 2) квалифицированный и эффективный ядерный регулирующий орган; 3) заинтересованные стороны, формирующие надежную институциональную основу и укрепляющие ее. Главную ответственность за обеспечение безопасности несет оператор, а главную ответственность за надзор за безопасностью – регулирующий орган. Заинтересованные стороны, которых может непосредственно затронуть авария, обеспечивают выполнение обязанностей в рамках других подсистем (в этой связи см. МАГАТЭ, «Основополагающие принципы безопасности» (2007 год)). У каждой подсистемы имеется важнейшая функция, и каждая из них способствует надлежащей работе остальных подсистем.

Структура этих трех подсистем в целом определяется правительством. Правительство должно обеспечить, чтобы для каждой системы были определены полномочия и обязанности, позволяющие выполнять четкие конкретные функции; при этом подсистемы должны быть связаны таким образом, чтобы работа каждой из них укрепляла и усиливала остальные подсистемы. Другими словами, правительство в законодательном порядке устанавливает обязательства лицензиата/оператора, создает и укрепляет регулирующий орган и с помощью законов, регулирующих доступ к информации, публичные слушания и юридические процессы оспаривания решений регулирующего органа, позволяет населению контролировать весь процесс.

Ниже описаны отдельные элементы этих трех подсистем.

Отраслевая подсистема. Лицензиат/оператор несет главную ответственность за обеспечение безопасности. Для этого используются внутренние процессы обзора безопасности со сложными системами сдержек и противовесов. К числу дополнительных уровней этой подсистемы относятся взаимодействие с отраслевыми партнерами на национальном и региональном уровне, взаимодействие с партнерами по отрасли на международном уровне (например, в рамках ВАО АЭС) и экспертиза международного уровня (например, миссии ОСАРТ МАГАТЭ). Для обеспечения эффективности этой подсистемы у лицензиата/оператора должна быть выстроена последовательная внутренняя концепция глубокоэшелонированной защиты. К числу ее элементов относятся: наличие мощного технического потенциала, в котором должности, связанные с безопасностью, заполняются компетентными сотрудниками, имеющими соответствующий опыт работы; наличие системы управления, предусматривающей множество проверок систем, связанных с безопасностью, и принятие соответствующих мер; независимый внутренний надзор за безопасностью, предполагающий независимые каналы представления информации высшему руководству (в том числе – в исключительных случаях – правлению); активный надзор за показателями безопасности; и стимулируемая руководством динамичная культура безопасности.

Подсистема регулирования. Подсистема регулирования должна иметь структуру с рядом уровней, аналогичную отраслевой подсистеме. К числу элементов, усиливающих регулирующие органы, относятся: 1) группы внешних экспертов по техническим вопросам (т.е. группы экспертов, консультирующих по вопросам природных опасностей, цифровых СКУ и другим сложным вопросам) и по процессу и проблемам менеджмента качества; 2) взаимодействие с международными партнерами (например, в рамках Конвенции о ядерной безопасности); 3) международные независимые экспертизы (например, миссии ИРРС МАГАТЭ).

Регулирующий орган должен располагать полномочиями, техническими знаниями и возможностями, позволяющими непрерывно обеспечивать защиту населения и окружающей среды. При этом в регулирующем органе обязательно должна быть налажена глубокоэшелонированная институциональная защита, в целом аналогичная по внутренней структуре механизмам лицензиата/оператора. Регулирующий орган должен подавать оператору пример того, как нужно стремиться к совершенствованию, учитывать внутреннюю и внешнюю критику и самостоятельно проводить критическое рассмотрение в целях повышения безопасности. В то же время регулирующему органу нужно взаимодействовать с заинтересованными сторонами, представляя им информацию, слушая и реагируя (см. «Привлечение заинтересованных сторон к решению ядерных вопросов» (Серия ИНСАГ, № 20, 2015 год)).

Подсистема заинтересованных сторон. Национальное правительство играет особую роль архитектора и организатора всей системы глубокоэшелонированной институциональной защиты, а также источника и способа воздействия на заинтересованные стороны. Среди уровней этой подсистемы – национальное правительство, местные органы, соседи, СМИ, группы по интересам и даже акционеры лицензиата/оператора *(см. там же)*.

Недостатки институциональной структуры оператора/лицензиата или регулирующего органа могут отрицательно сказаться на заинтересованных сторонах. Поэтому в общей системе привлечение заинтересованных сторон должно быть предусмотрено в качестве одного из средств соблюдения строгих норм ядерной безопасности и механизма обратной связи для коррекции недостатков других подсистем. Технических знаний населения может не хватать для того, чтобы сделать вывод о безопасности АЭС, однако полномасштабное информирование, честные и полные ответы на критику – это инструмент, позволяющий гарантировать выполнение обязательств лицензиатом/оператором и регулирующим органом *(см. там же)*.

Система в целом

Существует несколько аспектов системы ГэИЗ и связей между подсистемами, которые следует отметить:

- Каждая подсистема не зависит от других подсистем, но должна быть открытой и прозрачной для других подсистем. Внутри различных подсистем и между ними должна существовать эффективная связь.
- Для эффективной работы система в целом должна быть основательной. Все подсистемы и все слои и компоненты слоев должны быть прочными и функционировать эффективно.
- Одной из первостепенных обязанностей руководителей как в отрасли, так и в регулирующем органе является создание динамичной культуры безопасности. Эти культуры взаимосвязаны. То, каким образом отрасль реагирует на сигналы регулирующего органа, является отражением культуры, сложившейся в отрасли, и аналогичным образом то, как регулирующий орган выполняет свои обязанности, может влиять на культуру внутри отрасли.
- И отрасль, и регулирующий орган в качестве основополагающих ценностей должны проявлять открытость, прозрачность и подотчетность в отношении заинтересованных сторон. Вместо того чтобы просто представлять информацию, руководители отрасли и регулирующий орган должны приветствовать критику, исходящую от заинтересованных сторон, слушать, открыто реагировать, учиться и совершенствоваться. Только так можно добиться доверия у заинтересованных сторон.

* * *

В докладе ИНСАГ выражено мнение, согласно которому целостный подход к каждой из трех подсистем и взаимодействие между ними представляет собой один из тех аспектов ядерной безопасности, который ранее не рассматривался настолько комплексно, насколько этого требует данный вопрос. Хотя существующие международные механизмы обеспечения безопасности, такие как нормы безопасности и процессы независимой экспертизы, постоянно критически осмысливаются и совершенствуются, фукусимская авария свидетельствует о том, что эти процессы сами по себе еще не достаточны для создания прочной ГэИЗ.

Мы настоятельно призываем государства-члены воспользоваться следующими рекомендациями:

- МАГАТЭ должно разработать официальное руководство по ГэИЗ, охватывающее общую модель и три подсистемы.
- МАГАТЭ должно пересмотреть существующие нормы, руководящие материалы и механизмы независимой экспертизы с целью выявления пробелов во внедрении модели ГэИЗ.
- Это руководство должно стать основой для включения ГэИЗ в схему внешней проверки оператора, регулирующего органа и национальной инфраструктуры.
- Особое внимание следует уделять «странам-новичкам». Концепция ГэИЗ должна встраиваться в новую ядерную программу уже на раннем этапе.
- Следует подумать о том, чтобы предложить договаривающимся сторонам Конвенции о ядерной безопасности и Конвенции о безопасности обращения с отработавшим топливом сообщать об обеспечении ГэИЗ в рамках процедур рассмотрения.

Надеемся, что настоящее письмо пробудит интерес к готовящемуся докладу ИНСАГ. Как всегда, просьба обращаться ко мне во всех случаях, когда ИНСАГ может предложить помощь в этом или в других вопросах.

С уважением,

Искренне Ваш,
[Подпись]
Ричард А. Месерв

Копия: Х.К. Лентихо
Членам ИНСАГ