

УДК 621.039

О НЕКОТОРЫХ ТЕНДЕНЦИЯХ РЕГУЛИРОВАНИЯ ФИЗИЧЕСКОЙ ЯДЕРНОЙ БЕЗОПАСНОСТИ

Крупчатников Б.Н., советник директора ФБУ «НТЦ ЯРБ»

Признание того, что преднамеренные действия нарушителей могут быть причиной нежелательного радиационного воздействия на население, персонал и природную среду привело к созданию ряда международных механизмов, направленных на противодействие этой угрозе. В рамках МАГАТЭ была оформлена концепция физической ядерной безопасности, разработана обширная программа, в результате реализации которой была создана серия документов по физической ядерной безопасности с целью распространения передового опыта в странах, осуществляющих или намеревающихся осуществлять программы с использованием ядерных материалов и радиационных источников. Одной из форм практической реализации концепции физической ядерной безопасности стало внедрение понятия «физическая ядерная безопасность площадки». Непрерывный мониторинг угроз, отслеживание трендов и анализ национального опыта государств-участников позволили выработать подходы, направленные на комплексное решение вопросов, связанных с физической ядерной безопасностью. В работе представлено сопоставление механизмов регулирования, направленных на обеспечение физической безопасности, принятых в России, и современных тенденций, отраженных в документах МАГАТЭ. Приводятся соображения по поводу их возможной гармонизации с целью снижения рисков, связанных с событиями физической ядерной безопасности.

► **Ключевые слова:** физическая ядерная безопасность, физическая защита, ядерные материалы, несанкционированные действия, глубококошелолированная защита, модель нарушителя, интерфейс систем безопасности, эксплуатационная безопасность, риск неприемлемого радиационного воздействия.

ON NUCLEAR SECURITY REGULATION TRENDS

Krupchatnikov B., head advisor SEC NRS

Recognition that malicious acts by adversaries can cause the undesirable radiological effects on the population, personnel and the environment has led to creation of a number of the international mechanisms directed to counteraction to this threat. Within the IAEA concept of nuclear security the extensive program has been developed, as a result of which implementation of a series of documents on nuclear security for the purpose to share the best practices in the countries which are carrying out or intending to carry out programs with nuclear materials and radiation sources usage has been created. Introduction of "site nuclear security" concept became the practical form of implementation of the concept of physical nuclear security. Permanent monitoring of threats, tracking of trends and the analysis of national experience of the State Members has allowed to develop the approaches for the complex solution of the physical nuclear security issues. Comparison of the Russia's regulatory policies using in nuclear security, and the current trends reflected in documents of IAEA is given in work. Considerations regarding possible harmonization of them for the purpose to decrease the risks associated with nuclear security events are given.

► **Key words:** nuclear security, physical protection, nuclear material, malicious acts, defense in depth, design basic threat, safety-security systems interface, nuclear safety, inaccessible radiological effect risk.

Введение

Наличие ряда международных документов высшего уровня, таких как Конвенция о физической защите ядерного материала и ядерных установок, Международная конвенция по борьбе с актами ядерного терроризма, резолюции Совета Безопасности ООН 1373 и 1540, соглашения о международных гарантиях и дополнительных протоколах к ним, Кодекс поведения по обеспечению безопасности и сохранности радиоактивных источников, отражает тот факт, что опасность нежелательного радиационного воздействия от объекта использования атомной энергии на персонал, население и окружающую среду в результате злонамеренных действий лиц (потенциальных нарушителей) признается вполне реальной и значимой угрозой. Положения данных документов реализуются путем создания государственной инфраструктуры, призванной обеспечить защищенность ядерных и иных радиоактивных материалов и соответствующих объектов, на которых они используются, на территории государств и в пределах юрисдикции этих государств, а также противостоять попыткам использования указанных материалов в криминальных целях и их незаконному трансграничному обороту.

Главенствующую роль в выработке единых подходов на основании накопленного опыта в этой сфере и распространении наилучших практик среди государств, осуществляющих или намеревающихся осуществлять ядерные программы, играет МАГАТЭ. Следует отметить, что необходимость обеспечивать физическую ядерную безопасность МАГАТЭ рассматривает не только в отношении материалов и объектов, находящихся в рамках регулирующего контроля, но и в отношении ядерных и иных радиоактивных материалов, находящихся вне регулирующего контроля. Последнее в большей степени связано с хищением, утратой и незаконным оборотом ядерных и иных радиоактивных материалов и здесь не рассматривается.

1. Интерфейс ядерной и физической безопасности

Общий тезис о том, что целью государственной политики в области обеспечения ядерной и радиационной безопасности является последовательное снижение до социально приемлемого уровня риска техногенного воздействия на население и окружающую среду при использовании атомной энергии, содержится в [1] и указывает на важность интер-

фейса всех видов безопасности как фактора обеспечения безопасности в целом.

В отчете международной группы экспертов по ядерной безопасности INSAG-24 [2], посвященном вопросам интерфейса ядерной эксплуатационной безопасности и физической ядерной безопасности, обозначены различия в исходных событиях, влияющих на эксплуатационную ядерную безопасность и на физическую ядерную безопасность, при этом указывается, что конечная цель у них одна – снижение до приемлемого уровня рисков радиационного воздействия на персонал, население и окружающую среду. В отчете отмечается, что «основное внимание уделяется взаимосвязи между безопасностью и физической безопасностью на атомных электростанциях с целью обеспечения такого состояния, когда, по мере становления системы физической безопасности, обязательства по обеспечению безопасности и физической безопасности подкрепляли бы друг друга» [2].

Этому же вопросу, но в конкретной плоскости посвящена публикация [2], в которой рассматривается взаимосвязь аспектов ядерной безопасности и физической защиты на примере анализа того, как действия эксплуатационного персонала по управлению ядерной установкой могут быть организованы с учетом событий физической ядерной безопасности в свете концепции глубокоэшелонированной защиты. В частности, отмечается, что комплексное рассмотрение безопасности с учетом проектной угрозы (DBT – design basis threat) и применение подхода, определенного как «вероятностно-ориентированный детерминистский», позволит принять оптимальные проектные решения, снизить административную нагрузку и сократить ресурсы, предназначавшиеся ранее для решения вопросов физической защиты. Отмечается, что основой для разработки указанного подхода было признание того обстоятельства, что физическая защита является важной частью в системе глубокоэшелонированной защиты в ее традиционном понимании. Следующим логическим шагом был поиск аналогии с хорошо развитыми методами управления ядерной эксплуатационной безопасностью. В итоге методология, используемая для управления рисками таких событий, как пожар или наводнение, была признана применимой как некий «шаблон» для управления рисками событий, связанных с несанкционированными действиями. В качестве примера взаимного влияния эксплуатационной и физической ядерной безопасности приводятся результаты анализа ситуации с точки зрения того, обеспечивают ли

существующие меры физической защиты условия для продолжения нормальной эксплуатации блока АЭС или для его безопасного останова при различных сценариях действий нарушителей. При этом в учет принимаются меры не только по физической защите, но и по защите информации.

В российской регулирующей практике обеспечение ядерной и физической ядерной безопасности – в значительной степени независимые области. Тем не менее, определенный интерфейс регулирующих механизмов имеется и реализуется по следующим основным направлениям.

При нормативном регулировании – посредством того, что обязательные требования по вопросам физической ядерной безопасности общего характера, как правило, включаются в ФНП, устанавливающие требования к безопасности на всех этапах жизненного цикла, включая размещение, проектирование, создание, эксплуатацию и вывод из эксплуатации объекта использования атомной энергии, а также к отдельным видам деятельности в области использования атомной энергии. При этом детальные требования по вопросам физической ядерной безопасности издаются как отдельные специализированные документы (по учету и контролю, по физической защите ядерных материалов, ядерных установок и пунктов хранения, по физической защите радиоактивных веществ, радиационных источников, пунктов хранения радиоактивных веществ, радиоактивных отходов и пунктов хранения и захоронения радиоактивных отходов и иным специальным вопросам физической ядерной безопасности), в которых, в свою очередь, отражаются общие требования эксплуатационной ядерной безопасности в минимально необходимой степени.

Взаимосвязь между ядерной и радиационной и физической ядерной безопасностью осуществляется также при разработке и введении в действие ФНП по вопросам физической защиты, учета и контроля.

При лицензировании – посредством того, что в основном документе, регламентирующем деятельность, связанную с выдачей лицензий организациям, устанавливающим процедуры лицензирования деятельности в области использования атомной энергии, лицензионные требования по вопросам ядерной и радиационной и физической ядерной безопасности сбалансированы и гармонично сочетаются. При этом общие, рамочные, требования по вопросам физической ядерной безопасности включены практически во все разделы,

относящиеся к различным типам установок и видам деятельности. Детальные и подробные требования по физической безопасности для удобства и исключения многочисленного дублирования текста сформированы отдельными блоками в силу того, что эти требования универсальны и применимы к различным типам установок и видам деятельности.

Регламент предусматривает рассмотрение и экспертную оценку документов, обосновывающих возможность лицензиата обеспечить безопасность при осуществлении заявляемого вида деятельности. При этом для всех видов деятельности требуется обосновывать достаточность мер по обеспечению ядерной и радиационной безопасности и физической ядерной безопасности.

Частью лицензионного процесса является лицензирование персонала.

Руководители и специалисты, в обязанности которых входят вопросы исключительно физической ядерной безопасности, должны иметь общее представление и базовые навыки по вопросам радиационной и (или) ядерной безопасности, где это необходимо.

При осуществлении государственного надзора – посредством того, что государственный федеральный надзор за ядерной, радиационной, технической и пожарной безопасностью на объектах использования атомной энергии, за физической защитой ядерных установок, радиационных источников, пунктов хранения ядерных материалов и радиоактивных веществ, за системами единого государственного учета и контроля ядерных материалов, радиоактивных веществ, радиоактивных отходов, исполнением обязательных требований по аварийной готовности, защите информации, профессиональной подготовке и поддержанию квалификации соответствующего персонала осуществляется в форме комплексного взаимоувязанного и согласованного процесса.

2. Глубокоэшелонированная система физической ядерной безопасности объекта

В [1] отмечается, что изначально основное внимание уделялось лишь вопросам эксплуатационной безопасности, но в связи с расширением представлений о природе явлений и процессов, определяющих риски радиационного воздействия объектов использования атомной энергии, изменяется отношение к вопросам физической ядерной безопасности. Озабоченность вопросами распространения ядерного оружия привела к созданию системы

международных гарантий, в рамках которой большинство стран-участников МАГАТЭ создали свои национальные системы государственного учета и контроля ядерных материалов. Конвенция о физической защите ядерного материала и Конвенция о противодействии актам ядерного терроризма также отражали озабоченность в отношении тех последствий, которые могут иметь диверсии и хищения ядерных материалов. После известных террористических атак в США 11 сентября 2001 г. внимание к вопросам защищенности ядерных и радиационно опасных объектов резко возросло. Результатом этого стала активизация деятельности МАГАТЭ по разработке концепции физической ядерной безопасности и создание серии документов, охватывающих многочисленные аспекты этой области. Понятие «физическая ядерная безопасность» оказалось универсальной оболочкой, в рамках которой осуществлялось, осуществляется и будет осуществляться в дальнейшем деятельность, направленная на снижение до приемлемого уровня риска, проистекающего из преднамеренных противоправных действий в отношении объектов использования атомной энергии.

Следует отметить, что, как указывается в [4], концепция физической ядерной безопасности пришла на смену той концепции, которая ранее обозначалась как «физическая защита». При этом физическая защита как термин используется, в основном, в Конвенции о физической защите ядерного материала и ядерных установок и в относящихся непосредственно к этой Конвенции документах. Одной из форм практической реализации концепции физической ядерной безопасности является использование понятия «физическая ядерная безопасность площадки».

В документах МАГАТЭ, в частности в [5], говорится о необходимости оформления всего перечня мероприятий по обеспечению физической ядерной безопасности объекта в форме плана физической безопасности площадки (ПФБП) или эквивалентного набора документов. Следует отметить, что понятие «физическая безопасность площадки» включает ряд вопросов, которые в нашей терминологии определены как физическая защита, учет и контроль, информационная безопасность, антитеррористическая защищенность и культура безопасности. В [5] отмечается, что развитие технологий сопряжено с появлением новых угроз, которые должны своевременно выявляться и должным образом учитываться.

Известно, что общепринятым подходом обеспечения физической ядерной безопасности является построение системы безопасности на основе определения того, что защищается, от кого защищается и с какой целью [6]. Реализуется этот подход путем использования методологии оценки угрозы и масштабов последствий, анализа уязвимости объекта или вида деятельности и оценки эффективности (достаточности) принимаемых защитных мер. Одним из принципов построения системы физической ядерной безопасности является применение концепции глубокоэшелонированной защиты. Несмотря на то, что цели и мотивация потенциального нарушителя предполагаются неоднородными, меры или «барьеры» в рамках глубокоэшелонированной системы физической ядерной безопасности являются универсальным и включают следующие механизмы: административные, инженерные и технические, действия сил реагирования и культуру физической ядерной безопасности. Функциональными задачами глубокоэшелонированной системы физической ядерной безопасности полагаются: предупреждение, своевременное обнаружение, замедление продвижения или затруднение действий нарушителя, нейтрализация нарушителя или лишение его возможности осуществлять противоправные действия, а также ликвидация последствий.

3. Роль регулятора в установлении интерфейса систем, обеспечивающих физическую ядерную безопасность объекта

Система физической ядерной безопасности призвана обеспечить настолько низкий уровень рисков, связанных с несанкционированными действиями, чтобы их вклад не приводил к превышению уровня рисков радиационного воздействия, источником которых является ядерный или радиационно опасный объект, выше уровня, определяемого как неприемлемый. Как отмечалось в начале статьи [3], наиболее целостной моделью анализа безопасности могла бы быть модель, использующая методологию ядерной безопасности, но учитывающая в качестве факторов внешнего воздействия события, связанные с несанкционированными действиями нарушителей. Главным аргументом против практического использования указанного подхода и фактором, сдерживающим его практическую реализацию в настоящее время, является отсутствие достоверной статистики в отношении событий физической ядерной безопасности

и неопределенности, связанные с характеристиками модели нарушителей и ее гипотетическим характером. В связи с этим в настоящее время отсутствует постановка данной задачи в общей формулировке. Тем не менее, уже можно говорить о том, что сформировался подход к комплексному рассмотрению отдельного блока вопросов в рамках концепции физической ядерной безопасности.

Обращаясь вновь к [4], где указывается, что оператору надлежит предоставить на рассмотрение регулятора план физической ядерной безопасности площадки или эквивалентный набор документов, следует отметить, что в российской практике таким эквивалентным набором документов можно считать документы по физической защите и по учету и контролю. Однако их «эквивалентность» плану физической ядерной безопасности не является очевидной по ряду причин, среди которых можно указать неоднородность состава требований и различия в способах их формирования.

1. Требования к физической защите и учету и контролю устанавливаются в соответствии с процедурами, предусмотренными в рамках законодательства об использовании атомной энергии, а именно, в федеральных нормах и правилах, которые вводятся в действие органом регулирования безопасности при использовании атомной энергии, в то время как вопросы антитеррористической защищенности и информационной безопасности регулируются, соответственно, в рамках законодательства о противодействии терроризму [7] и о защите информации [8].

2. Требования к защите информации имеют свою специфику. В сфере информационной безопасности атомный объект подвержен специфическим угрозам, связанным с конфиденциальностью данных, в первую очередь, относящихся к вопросам физической безопасности, – физической защите, учету и контролю и антитеррористической защищенности. Несанкционированный доступ к информации и нарушение работы компьютеров и иных технических средств может повлечь за собой нарушение работы не только технологического оборудования, но и технических средств физической защиты, а также систем учета и контроля с целью совершения диверсии или незаконного изъятия материала. И наоборот, элементы информационных систем и соответствующее оборудование могут быть квалифицированы как предметы физической защиты, то есть являться объектами, на защиту которых направлена система физической защиты.

3. Требования к оценке последствий несанкционированных действий в рамках физической защиты, антитеррористической защищенности и информационной безопасности различны. Если в сфере закона об использовании атомной энергии это масштабы радиационного воздействия – производственный участок, территория объекта, санитарно-защитная зона, то для последствий, связанных с событиями информационной безопасности, это масштабы федерального, межрегионального, регионального, муниципального или локального уровня, вопросы антитеррористической защищенности, содержащие понятия защищенности инфраструктуры, социальной значимости, влияния и другие факторы, выходящие за рамки понятия «радиационные последствия».

4. Планы действий по ликвидации последствий и действий в чрезвычайных ситуациях, касающиеся вопросов физической защиты, не вполне увязаны со спецификой планов действий в режиме антитеррористической операции.

5. Требования к оценке эффективности сформулированы только в отношении системы физической защиты, но не установлены для иных, указанных выше подсистем физической ядерной безопасности. В связи с этим затруднительно перенести на систему учета и контроля или применить к комплексу мер по антитеррористической защищенности или мер информационной безопасности правило оценивать необходимость усовершенствования системы или комплекса мер на основе оценки их эффективности, или использовать оценку эффективности как инструмент оценки достаточности компенсирующих мероприятий. Имеет место некоторая неоднозначность в определении функциональности, так, например, в рамках системы физической защиты нарушитель с террористическими намерениями является частным случаем нарушителя, для противодействия которому предназначена система физической защиты, в то же время требования к антитеррористической защищенности рассматривают физическую защиту как один из инструментов обеспечения антитеррористической защищенности. При этом ответственности и ресурсов эксплуатирующей организации может оказаться недостаточно для проведения всего комплекса мероприятий по обеспечению антитеррористической защищенности ядерного объекта.

Различия наблюдаются также и в законодательстве, регулирующем осуществление надзора в указанных областях, относящихся к различным направлениям физической ядерной безопасности.

Приведенные выше моменты заслуживают более детального и глубокого анализа с позиции того, насколько существующие подходы регулирования физической ядерной безопасности способны адаптироваться к изменяющемуся характеру угроз и насколько реализуема цель удержания риска на уровне ниже того, который должен быть определен как общественно неприемлемый.

Выводы

В качестве основных направлений усовершенствования механизмов регулирования безопасности при использовании атомной энергии, целью которых является снижение рисков, связанных с преднамеренными (злонамеренными) действиями в отношении объектов использования атомной энергии, можно указать следующие:

- формирование подхода к построению системы регулирующих требований к физической безопасности площадки на основе комплексного учета угроз от событий, связанных с физической защитой, учетом и контролем, информационной безопасностью, человеческим и иными факторами;
- реализация риск-ориентированного подхода в регулировании путем разработки мето-

логии установления критериев эффективности соответствующих систем, относящихся к системам обеспечения физической ядерной безопасности на основе формирования критерия «неприемлемости» радиационных последствий;

- введение в нормативный лексикон российской нормативной базы по вопросам физической защиты, учета и контроля, антитеррористической защищенности, информационной безопасности и другим вопросам, касающимся защищенности объектов использования атомной энергии от преднамеренных противоправных действий, понятий, используемых в документах МАГАТЭ по физической ядерной безопасности, гармонизация подходов, используемых при регулировании физической ядерной безопасности, и подходов, используемых при формировании требований к обеспечению антитеррористической защищенности объектов использования атомной энергии;
- совершенствование методической базы по вопросам обеспечения физической ядерной безопасности (включая руководства по безопасности в области физической защиты, учета и контроля, информационной безопасности и иным вопросам в указанной сфере), методической базы по вопросам регулирования (нормативного регулирования, лицензирования и надзора).

Список литературы

1. Основы государственной политики в области обеспечения ядерной и радиационной безопасности Российской Федерации на период до 2025 г. Утверждены Президентом РФ 1 марта 2012 г. № Пр-539.
2. The Interface Between Safety And Security At Nuclear Power Plants INSAG-24. A report by the International Nuclear Safety Group International Atomic Energy Agency Vienna, 2010.
3. Safety Analysis In Design And Assessment Of The Physical Protection Of The OKG NPP P. Lindahl P. LINDAHL OKG Aktiebolag, Oskarshamn, Sweden Email: IAEA-TECDOC-CD-1749 International Conference on Topical Issues in Nuclear Installation Safety: Defence in Depth — Advances and Challenges for Nuclear Installation Safety Proceedings of an International Conference Held in Vienna, Austria, 21 – 24 October 2013.
4. Цель и основные элементы государственного режима физической ядерной безопасности. МАГАТЭ, Вена, 2014 STI/PUB/1590 ISBN 978–92–0–404814–8 ISSN 1816–9317.
5. Компьютерная безопасность на ядерных установках. МАГАТЭ, Вена, 2012 STI/PUB/1527 ISBN 978–92–0–435510–9 ISSN 1816–9317.
6. Рекомендации по физической ядерной безопасности, касающиеся физической защиты ядерных материалов и ядерных установок (INFCIRC/225/REVISION 5). МАГАТЭ, Вена, 2012 STI/PUB/1481 ISBN 978–92–0–424110.
7. Об антитеррористической защищенности объектов (территорий). Утверждено постановлением Правительства Российской Федерации от 25 декабря 2013 г. № 1244.
8. Об информации, информационных технологиях и о защите информации. Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 25.11.2017).

References

1. State Policy Fundamentals of the Russian Federation in the Field of Nuclear and Radiation Safety up to 2025. Approved by the Presidential Decree No. Pr-593 of March 1, 2012.
2. The Interface Between Safety and Security at Nuclear Power Plants INSAG-24. A report by the International Nuclear Safety Group International Atomic Energy Agency Vienna, 2010.
3. Safety Analysis in Design and Assessment of the Physical Protection of the OKG NPP P. Lindahl P. LINDAHL OKG Aktiebolag, Oskarshamn, Sweden Email: IAEA-TECDOC-CD-1749 International Conference on Topical Issues in Nuclear Installation Safety: Defence in Depth – Advances and Challenges for Nuclear Installation Safety Proceedings of an International Conference Held in Vienna, Austria, 21 – 24 October 2013.
4. Objective and Essential Elements of a State's Nuclear Security Regime. IAEA, Vienna, 2014 STI/PUB/1590 ISBN 978-92-0-404814-8 ISSN 1816-9317.
5. Computer Security at Nuclear Facilities. IAEA, Vienna, 2012 STI/PUB/1527 ISBN 978-92-0-435510-9 ISSN 1816-9317.
6. Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/REVISION 5). IAEA, Vienna, 2012 STI/PUB/1481 ISBN 978-92-0-424110.
7. On Anti-Terrorism Security of the Facilities (Territories). Approved by the Decree of the Government of the Russian Federation No. 1244 dated of December 25, 2013.
8. On Information, Information Technologies and Protection of Information. Federal Law No. 149-FZ dated of 27.07.2006 (Rev. of 25.11.2017).

