

УДК 621.039.58

ФИЗИЧЕСКАЯ ЗАЩИТА АЭС

Г.В. Токмачев

Нормативная база МАГАТЭ

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

Вопросам физической защиты от несанкционированного изъятия ядерного материала и от саботажа в отношении ядерного материала и ядерных установок посвящен ряд недавних публикаций МАГАТЭ [1—3]. В них даются общие рекомендации по проектированию и оценке защитных мер. Кроме того, МАГАТЭ разработало программу подготовки специалистов по физической защите АЭС [4].

Для достижения наиболее высокого уровня уверенности в физической защите требуется тесная корреляция между защитными мерами и угрозами. Этот подход базируется на основополагающем принципе, который заключается в том, что физическая защита ядерных ресурсов, находящихся под юрисдикцией государства, должна основываться на проведенной государством оценке угроз этим ресурсам.

Базовым понятием физической защиты является концепция модели нарушителя (*design basis threat — DBT*) [1]. Модель нарушителей — всесторонняя совокупность сведений о мотивации нарушителей и преследуемых ими целях, численности, оснащенности, подготовленности и тактике действий, которые используются при выработке требований к системе физической защиты и оценке ее эффективности.

Необходимо, чтобы концепция модели нарушителя была внедрена в регулирующую деятельность и использовалась для следующих целей в отношении системы физической защиты:

- разработки технических требований;
- определения проектных критериев;
- установления критериев оценки;

- разграничения сфер ответственности государства и эксплуатирующей организации.

Внедрение концепции модели нарушителя в регулирующую деятельность позволит управлять рисками от враждебной деятельности путем разработки надлежащих мер и систем физической защиты. Это должно сопровождаться оценкой существующих систем физической защиты, проводимой регулирующим органом, чтобы убедиться, что они эффективны против модели нарушителя. При этом концепция модели нарушителя используется как основа для разработки потенциальных сценариев совершения враждебных актов, анализа эффективности системы физической защиты и ее уязвимости, улучшения системы (если необходимо), анализа и приоритезации мероприятий по модернизации с точки зрения их эффективности и затрат на реализацию.

Для того чтобы оценка угроз эффективно использовалась в качестве базиса для разработки системы физической защиты, необходимо тесное взаимодействие организаций, имеющих опыт в различных областях деятельности. Это, например, организации, имеющие опыт сбора разведанных, но ограниченные знания установок и материалов, которые необходимо защитить, и организации, в частности, надзорный орган, знакомые с эксплуатационными условиями и стратегиями защиты, но неопытные в оценке угроз.

Процесс анализа угроз не предусматривает определение специфических сценариев нападения потенциального нарушителя, а должен быть нацелен на правдоподобную оценку его характеристик. Характеристики включают мотивацию, намерения, состав группы, виды вооружений и взрывчатых веществ, инструменты, способ транспортировки, навыки, в том числе компьютерные, знания обстановки, финансирование, поддерживающие структуры, тактику.

Система физической защиты радиоактивных источников должна проектироваться для выполнения следующих базовых функций [2]: предупреждение несанкционированных действий, их своевременное обнаружение, задержка

(замедление) проникновения нарушителя, реагирование на несанкционированные действия и управление безопасностью объекта. Управление безопасностью включает наличие адекватных ресурсов (персонала и финансов), процедур, планов, обеспечение культуры безопасности и информационной безопасности.

Хорошо спроектированная система физической защиты должна соответствовать следующей концепции:

- эффективность предупреждения несанкционированных действий не может быть оценена количественно, поэтому физическая защита не может быть полностью основана на этой функции;

- обнаружение несанкционированных действий должно предшествовать их задержке для того, чтобы обеспечить персонал физической защиты достаточным резервом времени на реагирование. Если нарушитель успеет раньше преодолеть физический барьер, что является самой трудной задачей, то он будет иметь большие шансы совершить диверсионный акт или хищение радиоактивного источника. В этом случае физический барьер выполняет только функцию предупреждения, а не задержки;

- обнаружение нарушителя должно всегда сопровождаться анализом и определением причин подачи сигнала тревоги средством обнаружения. Для этого могут использоваться системы дистанционного видеонаблюдения;

- время, в которое осуществляется задержка нарушителя, должно превышать сумму периодов времени, требуемых на оценку ситуации и реагирование на несанкционированные действия;

- физическая защита должна быть сбалансирована, то есть должна обеспечить адекватную защиту (время задержки, меры по обнаружению, реагирование) от всех угроз через все возможные пути проникновения нарушителя;

- должна быть обеспечена глубоко эшелонированная защита, концепция которой предусматривает наличие нескольких уровней и методов физической защиты (конструкционный, технический, человеческий и организационный).

Проект системы физической защиты должен соответствовать угрозам, определенным в модели нарушителей, и базироваться на следующем:

- контроль доступа может осуществляться через контрольно-пропускные пункты, контролируемые службой безопасности, с помощью электронных считывающих устройств или ключей;

- металлические клетки или контейнеры могут использоваться для физического разделения или изоляции охраняемых источников, что обеспечивает задержку проникновения нарушителя в охраняемую зону;

- система видеонаблюдения является полезным средством, которое позволяет персоналу физической защиты контролировать внешние подходы и охраняемые зоны. Камеры могут комбинироваться с системами контроля проникновения и тревожно-вызывной сигнализацией;

- персонал службы безопасности должен быть обеспечен эффективными и надежными видами связи между такими основными звеньями, как патруль, караул, центр управления, а также с внешними спецслужбами, ответственными за быстрое реагирование в случае несанкционированного действия;

- защитные ограждения вдоль охраняемого периметра должны соответствовать угрозам и охраняемому предмету физической защиты, а также категории охраняемой зоны в целом. Ворота должны проектироваться по стандартам, сравнимым со стандартами для защитных ограждений, и оборудоваться замками высокого качества;

- системы обнаружения проникновения являются полезным средством контроля безопасности необслуживаемых зон. Система охранной сигнализации может срабатывать дистанционно на посту охраны или по месту посредством звукового сигнала большой громкости. Система видеонаблюдения может быть полезным средством первоначальной оценки ситуации в этой зоне, но должна дублироваться визуальной проверкой, осуществляемой патрульной службой;

- ключи, которые позволяют осуществить доступ к радиоактивным источникам, должны контролироваться и находиться на ответственном хранении;

- замки, используемые для защиты радиоактивных источников, должны быть хорошего качества и обеспечивать определенное сопротивление насильственным действиям. Такие же требования предъявляются к дверным петлям. Блокировки дверей могут помочь службе безопасности контролировать перемещения персонала и его доступ к предмету физической защиты;

- запертые защищенные контейнеры с радиоактивными веществами могут обеспечить защиту и задержку несанкционированных действий. При этом необслуживаемые помещения также должны быть оборудованы тревожно-вызывной сигнализацией;

- система контроля несанкционированного доступа должна проверяться как при установке, так и при эксплуатации через определенные интервалы. Также периодически должно проводиться техническое обслуживание системы;

- пропускная система должна обеспечивать идентификацию владельца пропуска;

- система физической защиты должна удовлетворять стандартам обеспечения качества;

- эффективное освещение охраняемой зоны может быть важным фактором физической защиты;

- внутри определенных зданий возможна установка дополнительных защитных дверей, затрудняющих несанкционированный доступ к объекту физической защиты;

- система физической защиты должна продолжать выполнять свои функции в случае обесточивания охраняемой зоны. Для этой цели могут быть предусмотрены резервный дизель-генератор, который автоматически запускается при потере напряжения, и аккумуляторные батареи, которые могут рассматриваться только в качестве кратковременного источника энергии;

- стены являются дорогим способом формирования охраняемого периметра. Кроме того, к их недостатку следует отнести невозможность визуального наблюдения за пределами охраняемой зоны.

Анализ уязвимости — метод оценки системы физической защиты. Его существенными элементами являются следующие:

- определение состава радиоактивного источника, его характеристик, расположения и окружающей обстановки;

- оценка потенциальных последствий, связанных с хищением, несанкционированным использованием или диверсией;

- анализ национальной модели нарушителей и местной обстановки;

- определение существующих мер защиты и оценка их ожидаемой эффективности при нападении нарушителей, постулируемых моделью;

- определение дополнительных мероприятий, если необходимо, для обеспечения приемлемого и соразмерного уровня физической защиты.

Упомянутые выше документы МАГАТЭ в основном ориентированы на предупреждение внешних угроз. Кроме того, разработано руководство, посвященное теме внутренних нарушителей [3]. Угрозы, исходящие от внутренних нарушителей, создают проблему для систем физической защиты, которая радикально отличается

от других проблем. Внутренние нарушители могут использовать такие преимущества, как наличие у них прав доступа, полномочий и знание установки, которые могут позволить обойти специальные элементы физической защиты или другие предусмотренные меры. Кроме того, являясь сотрудниками, обладающими соответствующим доступом и пользующимися доверием в соответствии со своей должностью, внутренние нарушители имеют возможности для применения методов «нанесения ущерба», которыми не располагают внешние нарушители в случае, когда им приходится сталкиваться с элементами защиты и мерами контроля доступа. Внутренние нарушители имеют больше возможностей для выбора наиболее уязвимой цели и наиболее выгодного времени для совершения злоумышленного действия.

Подход к противодействию угрозе, исходящей от внутреннего нарушителя, предусматривает разработку конкретных предупредительных и защитных мер.

В качестве предупредительных рекомендуются следующие меры:

- проверка личности для подтверждения подлинности данного лица;

- оценка надежности, то есть начальная и дальнейшие непрерывные оценки добросовестности, честности и надежности лиц;

- сопровождение работников и посетителей, редко бывающих на объекте, и наблюдение за ними;

- осуществление хорошей программы информированности персонала и подрядчиков по вопросам физической безопасности;

- обеспечение конфиденциальности (безопасности информации);

- обеспечение качества всех видов деятельности, важных с точки зрения предупреждения и защиты от угроз;

- удовлетворенность служащих;

- физическое разделение зон доступа к установкам;

- разделение видов работы для ограничения способности внутренних нарушителей иметь необходимые потенциальные возможности для совершения злоумышленного действия;

- санкции (дисциплинарные меры и судебное преследование).

В качестве защитных мер рекомендуется следующее:

- выявление несанкционированных действий, что может осуществляться с помощью защитных датчиков, посредством наблюдения за

персоналом и/или мониторинга рабочих процессов. Правило двух лиц требует, чтобы по меньшей мере два опытных работника контролировали друг друга в чувствительной зоне. Отслеживание перемещения и мест нахождения персонала на объекте способствует обеспечению защиты от нарушения правил доступа, а также позволяет получить полезную информацию после инцидента;

- задержка действий в осуществлении замысла, которую обеспечивают персонал, процедуры или физические барьеры, что увеличивает время, требующееся нарушителю для совершения несанкционированных действий. Большинство барьеров проектируется так, чтобы они осуществляли задержку проникновения в помещения или зоны, а не задержку совершения злоумышленных действий. Таким образом, они обеспечивают лишь ограниченное противодействие внутренним нарушителям;

- реагирование на несанкционированное действие внутреннего нарушителя, которое могут осуществлять как сотрудники служб безопасности, так и эксплуатационный персонал;

- планы аварийных мероприятий, которые следует разрабатывать с целью возвращения похищенного ядерного материала и смягчения или сведения к минимуму радиационных последствий диверсии.

Физическая защита АЭС США

В публикации [5] отмечается, что отсутствие общественного давления в отношении дорогостоящих мероприятий по модернизации системы физической защиты АЭС является причиной того, что уровень таких систем является недостаточным. Атаки террористов становятся все изощреннее, что доказывают факты поразительно дерзких нападений на тщательно охраняемые объекты в Афганистане, Пакистане и Ираке.

Целью террористов может быть оборудование АЭС, повреждение которого может вызвать повреждение ядерного топлива в активной зоне или бассейне выдержки. Соответственно, основной целью физической защиты АЭС является предотвращение указанных последствий.

Проблема эффективной физической защиты в США заключается в том, что АЭС не проектировались для противодействия такому виду воздействий. Поэтому внешние электротехнические устройства или номинально независимые каналы систем безопасности, но недостаточно физически разделенные, могут быть удобной мишенью для действий террористов.

Комиссия по ядерному регулированию США (NRC) выпустила два норматива в отношении падения самолета. Первый требует от эксплуатирующих организаций разработки руководств по действиям при оповещении о воздушной угрозе и по противоаварийным мероприятиям при возможных потерях зданий и сооружений АЭС вследствие пожаров и взрывов. Второй норматив требует от компаний, запрашивающих лицензию на сооружение новой АЭС, оценки последствий падения тяжелого гражданского самолета на АЭС и внедрения дополнительных мер защиты, если необходимо, для обеспечения или целостности защитной оболочки, или отсутствия повреждения активной зоны реактора. По крайней мере, для двух новых проектов результаты анализа последствий падения самолета вызвали необходимость внесения изменений в проект АЭС.

Анализ проекта усовершенствованного кипящего реактора GE-Hitachi ABWR показал, что падение самолета не повреждает защитную оболочку и оборудование внутри нее, но здания реактора и систем управления могут не выдержать такого воздействия. Это может вызвать потерю вспомогательной питательной воды и аварийного охлаждения активной зоны. Поэтому в проект была дополнительно включена альтернативная система питательной воды.

Компания Westinghouse переработала проект защитной оболочки для того, чтобы удовлетворить более жестким требованиям стандарта по внешним воздействиям, связанным с падением самолета. Проект АЭС не был одобрен NRC, она потребовала проведения испытания для подтверждения того, что новая конструкция будет способна выполнять заданные функции безопасности.

В отношении защиты АЭС против наземного нападения в 2007 г. NRC выпустила новые правила формирования модели нарушителей, то есть специфических характеристик атакующей группы (модель нарушителя), против которой на АЭС должны быть предусмотрены защитные меры. Ранее постулировалось нападение группы из трех человек, не склонных к суициду, и наличие «пассивного» информатора, не участвующего в нападении. Теперь АЭС должна быть защищена от более широкого спектра угроз, включая большее число нападающих, более совершенное и разнообразное вооружение и повышенный размер передвижного взрывного устройства. Под давлением промышленности NRC приняла правила, в которых модель нарушителя дана в заметно более мягком варианте, чем ожи-

дали спецслужбы, утверждая, что защита против запроектных угроз является ответственностью правительства, а не частных компаний.

Проверка действенности стандартов физической защиты АЭС проводится путем организации нападений условного нарушителя на объекты АЭС, потеря которых может вызвать серьезное повреждение активной зоны реактора или облученного топлива в бассейне выдержки. Численность и вооружение нападающих выбирается в соответствии с действующими стандартами. Структуры, отвечающие за физическую защиту АЭС, должны отразить нападение. Такие проверки с установленной периодичностью 3—8 лет сейчас являются регулирующим требованием NRC. Кроме того, ужесточены требования NRC к тренировкам и квалификации сотрудников вооруженной охраны АЭС. Дело в том, что проводившиеся до терактов 11 сентября проверки показали, что группа террористов из трех человек смогла достичь своих целей почти в 50% нападений, несмотря на то, что руководство АЭС было предупреждено за месяц о готовившейся акции. В 2008 г., уже по новым нормативным требованиям, было проведено 24 условных нападения на АЭС США, с двумя из которых персонал физической защиты разных станций не справился. Кроме того, вооруженная охрана некоторых АЭС с большим трудом отразила возникшие угрозы. Поэтому в 2009 г. NRC начала разрабатывать более детальную систему аттестации физической защиты АЭС.

Другим важным аспектом является усталость сотрудников охраны станции, некоторые из которых работают до шести 12-часовых смен в неделю. Поэтому NRC предложила норматив по ограничению рабочего времени для персонала охраны (48 часов в неделю для 12-часовых смен при нормальной обстановке).

Руководитель NRC отметил, что концепция риска используется в регулирующей деятельности США с 1995 г., когда применение результатов вероятностных анализов безопасности стало рассматриваться как дополнение и усиление традиционного регулирования АЭС [6]. В настоящее время предлагается расширить сферу применения этих анализов на систематической основе на область физической защиты, так как пока подобные анализы риска применялись лишь эпизодически для оценки эффективности физической защиты. Основная трудность заключается в том, что такой риск трудно оценить количественно. С другой стороны, при отсутствии таких оценок NRC и промышленность про-

должают испытывать давление по поводу повышения уровня физической защиты, чтобы снизить риск до «нулевого» уровня, что невозможно достичь в любой человеческой деятельности. По мнению руководства NRC, физическая защита АЭС по многим аспектам достигла такого уровня, что введение новых требований не сильно ее улучшит. Не самым удачным примером реализации одного из требований является внедрение на АЭС пуленепробиваемых ограждений для наблюдательных постов и оборонительных позиций охраны. Эта мера повысила защищенность сотрудников охранных подразделений, но привела к снижению их внимательности, вызванному пребыванием персонала в тесных и слабо вентилируемых помещениях с обзором, ограниченным узкими прорезями в стенах.

Тем не менее нормативная документация NRC достаточно динамично изменяется. Одной из новых возникших проблем в области физической защиты АЭС является проблема угроз, связанных с компьютеризацией и передачей информации [7].

Бывший сотрудник ЦРУ отмечает следующие недостатки в подготовке личного состава охраны АЭС США [8]:

- ограниченное число охранников в смене (20 человек) для контроля всего периметра;
- недостаточный объем тренировок по обращению с оружием (2—3 раза в году);
- слишком краткая начальная тренировка, по крайней мере для лиц, не имеющих опыта военной службы (до недели, включая административные вопросы);
- низкий боевой дух охраны;
- ограниченность сценариев, используемых для тренировки персонала, и в плане малочисленности нападающих, и в отношении применяемого ими вооружения (без автоматического и реактивного оружия).

Список литературы

1. Development, use and maintenance of the design basis threat: implementing guide. — IAEA nuclear security series no. 10. Vienna: International Atomic Energy Agency, 2009.
2. Security of radioactive sources: implementing guide. IAEA nuclear security series no. 11. — Vienna: International Atomic Energy Agency, 2009.
3. Предупредительные и защитные меры в отношении угроз, исходящих от внутреннего нарушителя. Практическое руководство. Серия изданий МАГАТЭ по физической ядерной безопасности, № 8, МАГАТЭ, Вена, 2009 г.

4. Educational programme in nuclear security: technical guidance. IAEA nuclear security series no. 12. — Vienna: International Atomic Energy Agency, 2010.
5. E.S. Lyman. Security since September 11th. — Nuclear Engineering International, 2010, v. 55, No 668, p. 14—19.
6. D.K. Raleigh. Risk Management and Security. Grand Challenge Summit 2010 North Carolina State University Raleigh, North Carolina. NRC, No. S-10-006, March 5, 2010. <http://www.nrc.gov/reading-rm/doc-collections/commission/speeches/2010/s-10-006.html>.
7. G.B. Jaczko. Regulation and the Future of Nuclear Science and Technology. American Nuclear Society Annual Meeting. San Diego, CA. NRC, No. S-10-018, June 14, 2010.

- <http://www.nrc.gov/reading-rm/doc-collections/commission/speeches/2010/s-10-018.html>.
8. C.S. Faddis. Nuclear plants need real security. CNN, March 15, 2010. <http://edition.cnn.com/2010/OPINION/03/15/faddis.nuclear.plant.security/index.html>.

Ключевые слова

Атомная станция, физическая защита, МАГАТЭ, модель нарушителя, внешний нарушитель, внутренний нарушитель, несанкционированные действия.

Тройственное соглашение по быстрым реакторам

Комиссариат по атомной и альтернативным источникам энергии Франции (СЕА), Агентство по атомной энергии Японии (JAEA) и Министерство энергетики США (DoE) опубликовали совместное заявление о трехстороннем сотрудничестве в области разработки реакторов на быстрых нейтронах с натриевым теплоносителем (SFR), которое является дополнением к меморандуму о взаимопонимании от 2008 г.

Меморандум предполагает «непрерывную координацию работ», осуществляемых JAEA, СЕА и DoE по разработке концепции прототипной/демонстрационной установки SFR в соответствии с программными целями по развитию атомной энергетики каждой из стран. В рамках соглашения процесс разработки SFR реализуется за счет «прямого сотрудничества организаций-разработчиков технологии» стран-участниц проекта. У Франции и Японии уже имеются четкие графики строительства установок SFR. В частности, Франция предполагает к 2020 г. ввести в Маркуле демонстрационный реактор на быстрых нейтронах (с натриевым охлаждением) «Астрид» мощностью 600 МВт эл. Текущие работы в Соединенных Штатах направлены на проведение оценки системы, конструкционных материалов, анализ безопасности и возможностей SFR в части обращения с облученным ядерным топливом. Кроме того, в рамках действующего соглашения JAEA, СЕА и DoE обсуждают общие проектные требования, проводят сравнение реакторных установок различных типов, а также технологий и объектов, позволяющих реализовать сотрудничество в области НИОКР применительно к будущим SFR.

Партнеры намерены осуществлять обмен информацией и начать сотрудничество по гармонизации работ в области SFR путем «выявления взаимодополняющих направлений НИОКР», связанных с реакторами на быстрых нейтронах

и соответствующими технологиями топливного цикла. С целью продвижения работ по созданию SFR соглашение дополнено новыми направлениями сотрудничества. Подписавшие меморандум ведомства планируют совместно использовать эксплуатационные и экспериментальные данные, собранные на реакторах: Joyo и Monju (Япония), Phenix и Superphenix (Франция), EBR-II и FFTF (США).

По условиям соглашения стороны рассмотрят вопрос о целесообразности совместной фабрикации топлива для быстрых реакторов.

Все три организации уже сотрудничают в рамках Международного форума «Поколение IV».

Действующие и сооружаемые реакторы на быстрых нейтронах в мире

| Страна, реактор | МВт эл. | Начало эксплуатации |
|-----------------|-----------|---------------------|
| | МВт тепл. | |
| Россия | | |
| БОР-60 | 12 | 1969 |
| БН-600 | 600 | 1980 |
| БН-800 | 800 | 2014 (по плану) |
| Япония | | |
| Joyo | 140 | 1977 |
| Monju | 280 | 1994—1995; 2010 |
| Индия | | |
| FBTR | 40 | 1985** |
| PFBR | 500 | 2012** |
| Китай | | |
| CEFR | 20 | 2010*** |

* Все — с натриевым теплоносителем.

** FBTR — Fast Breeder Test Reactor, в Калпаккаме, 18 октября с.г. исполнилось 25 лет с момента достижения первой критичности, успешный опыт его эксплуатации заложил основу для строительства блока с энергетическим быстрым реактором PFBR, ввод в строй которого перенесен с 2010 на 2012 г.

*** Достиг критичности в июле 2010 г.

*Материал подготовила И.В. Гагаринская
 Новости. Ядерная энергия, человек,
 окружающая среда. РНЦ «Курчатовский
 институт», октябрь 2010 г.*