ЗАЩИТА СИСТЕМЫ ФИЗИЧЕСКОЙ ЗАЩИТЫ ОБЪЕКТОВ ИСПОЛЬЗОВАНИЯ АТОМНОЙ ЭНЕРГИИ ОТ НЕСАНКЦИОНИРОВАННЫХ ДЕЙСТВИЙ

А. А. Дашкевич

Учреждение образования «Военная академия Республики Беларусь», г. Минск

Научный руководитель А. М. Кузьмицкий

На заседании Совета безопасности Республики Беларусь, которое проходило 15 января 2007 г. под председательством главы государства, было принято окончательное решение о собственной атомной электростанции. Сегодня строительство Бе-

лорусской АЭС находится на завершающей стадии. При этом атомная электростанция является особо важным государственным объектом, который должен обладать соответствующей защищенностью.

На вопрос, что именно надо защищать, отвечает определение, приведенное в Законе Республики Беларусь «Об использовании атомной энергии» (принят 30 июля 2008 г.): «объекты использования атомной энергии (ОИАЭ) – ядерная установка, пункт хранения, ядерные материалы, отработавшие ядерные материалы, эксплуатационные радиоактивные отходы».

Для обеспечения безопасности АЭС создается система физической защиты (СФЗ). Определения понятий «физическая защита» (ФЗ), «системы физической защиты» и «эффективность системы физической защиты» закреплены в ТКП 531–2014.

Так, ФЗ – это комплекс технических, организационных и иных мер, направленных на сохранность ОИАЭ и предотвращение несанкционированного доступа к ним; СФЗ – это совокупность организационных и технических мероприятий, проводимых администрацией ядерного объекта, его службой безопасности, подразделениями охраны (персоналом СФЗ) с использованием инженерно-технических средств физической защиты.

Эффективность СФЗ – ее способность противостоять действиям нарушителей в отношении ядерных материалов, ядерных установок, пунктов хранения и (или) других предметов ФЗ с учетом принятого при проектировании СФЗ перечня угроз и моделей нарушителей.

В целях формирования единого подхода к определению угроз в отношении ОИАЭ, учитываемых при создании СФЗ в Республике Беларусь, в 2010 г. министром внутренних дел было утверждено Положение о проектной угрозе объектам использования атомной энергии, в котором были определены следующие обобщенные типы нарушителей:

I – внешний нарушитель – террористическая или диверсионная группа. Вероятная тактика действий – насильственная, с вооруженным нападением, преодолением физической защиты ОИАЭ (в том числе с применением транспортных средств), с возможным захватом заложников.

II – внешний нарушитель, преследующий корыстные цели. Вероятная тактика действий – скрытая. Может вступать в сговор с личным составом подразделений охраны с целью получения информации и проникновения на ОИАЭ.

III – внутренний нарушитель – сотрудник ОИАЭ из числа обслуживающего персонала, имеющий право доступа на территорию и внутрь вспомогательных сооружений, но не имеющий права постоянного доступа к местам хранения ядерных материалов и технологическому оборудованию, несанкционированные действия в отношении которого могут привести к аварии на АЭС. Вероятная тактика действий – скрытая.

IV – внутренний нарушитель – сотрудник ОИАЭ, имеющий непосредственный доступ к ФЗ ОИАЭ. В остальном характеризуется как нарушитель третьего типа. Вероятная тактика действий – скрытая. Возможно перемещение ядерных материалов за пределы места их хранения с последующим выносом за территорию объекта (скрыто или по подложным документам).

V – внутренний нарушитель – работник (военнослужащий) подразделения охраны или сотрудник службы безопасности ОИАЭ. Вероятная тактика действий – скрытая, в том числе с отключением технических средств ФЗ ОИАЭ.

Для ответа на вопрос, как защищать, рассмотрим инженерные и технические средства ФЗ, которые препятствуют несанкционированным действиям нарушителя.

К инженерным средствам ФЗ относятся сооружения, конструкции и физические барьеры. Под физическим барьером следует понимать препятствие, создающее задержку по времени проникновению нарушителя в охраняемые зоны: к уязвимым местам или ядерным материалам.

Физическими барьерами являются: строительные конструкции ядерного объекта (стены, перекрытия, ворота, двери); специально конструкции (заграждения, противотаранные устройства, решетки, усиленные двери, контейнеры); другие физические (в том числе естественные) препятствия.

Техническими средствами системы физической защиты являются элементы и устройства, входящие в состав следующих основных функциональных систем: охранной и тревожно-вызывной сигнализации; контроля и управления доступом; оптико-электронного наблюдения и оценки ситуации; оперативной связи и оповещения; защиты информации; телекоммуникаций; обеспечения электропитания, освещения.

Таким образом, основными средствами, затрудняющими действия нарушителей при попытках несанкционированного проникновения, являются физические барьеры. Обнаружение несанкционированного доступа в охраняемые зоны, здания, сооружения, помещения и выдачу сигнала о срабатывании средств обнаружения обеспечивает охранная и тревожно-вызывная сигнализация.

Расчеты, необходимые для определения и оценки эффективности СФЗ и уязвимости ОИАЭ, требуют учета многочисленных данных и факторов и, как следствие, значительных трудозатрат. Применение компьютерного моделирования для оценки эффективности как проектируемой, так и существующей СФЗ позволяет уменьшить объемы работы аналитика и свести к минимуму вероятность возможных ошибок.

Конечным результатом анализа является количественная характеристика эффективности, определяемая как вероятность преодоления нарушителем СФЗ, позволяющая понять, на каком этапе преодоления различных физических барьеров СФЗ окажется неэффективной (т. е. силы реагирования не успевают прибыть в определенное место до того, как нарушитель совершит задуманное). Это поможет в установлении и устранении ее слабых мест. В сущности задача оценки уязвимости является задачей вероятностного анализа и может быть решена известными способами.

Рассмотрим пример моделирования попытки совершения террористического акта и его предотвращения. Вооруженная *террористическая* группа прорывается через физические барьеры, установленные на периметре объекта. В момент T_0 (начало действий нарушителей) первое средство обнаружения выдает сигнал тревоги. В момент $T_с$ начинают действовать силы реагирования. Нарушитель последовательно преодолевает физические барьеры внутри охраняемой зоны.

Задержка завершается в момент $T_п$ и нейтрализация нарушителя завершает выполнение задачи в момент $T_з$ до совершения им несанкционированного действия и побега.

Сценарий действий нарушителя выглядит следующим образом (рис. 1):

– задача 1 – преодолеть физические барьеры на периметре объекта;

– задача 2 – проникнуть в охраняемое здание;

– задача 3 – проникнуть в охраняемое помещение;

– задача 4 – совершить несанкционированное действие и побег с объекта.

Общее время задержки нарушителя $T_{\min}$ рассчитывается по формуле

$$T_{\min} = \sum_{i=k}^{m} T_i > T_g,$$

где m – общее число физических барьеров, находящихся на маршруте движения нарушителя от начала запретной зоны до пункта хранения ядерных материалов; k – точка, в которой $T_{\min}$ начинает превышать T_g; i – средство обнаружения нарушителя; T_g – время выдвижения сил реагирования.

Суммарная вероятность обнаружения определяется по формуле

$$P_I = 1 - \prod_{i=k}^{k-1} (1 - P_i),$$

где P_I – вероятность обнаружения нарушителя датчиком обнаружения; $(1 - P_i)$ – вероятность необнаружения.

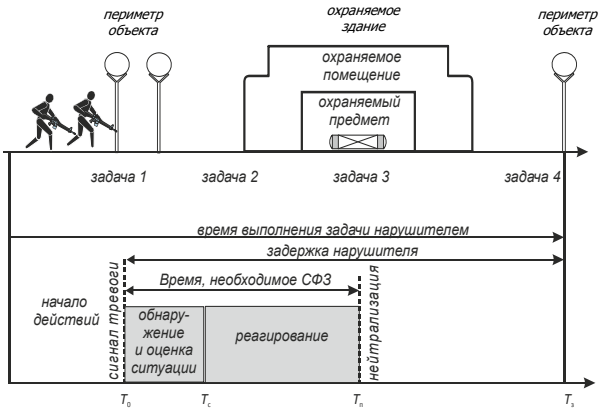

Рис. 1. К иллюстрации сценария действий нарушителя и сил реагирования

Сегодня при создании систем физической защиты применяются самые передовые технологии, в том числе и в области системного анализа и математического моделирования развития чрезвычайной ситуации. Представленный обзор программного обеспечения предопределяет два возможных направления деятельности специалистов, участвующих в обеспечении комплексной безопасности функционирования Белорусской АЭС.

Во-первых – изучение, выбор и использование наиболее оптимального из представленных программных продуктов в практической деятельности по оценке уязвимости системы физической защиты. Во-вторых – разработка собственных алгоритмов и программ системного анализа и оценки эффективности системы физической защиты.