

МЕЖДУНАРОДНАЯ ИНФОРМАЦИЯ

НАЦИОНАЛЬНАЯ ЛАБОРАТОРИЯ САНДИЯ ПРЕДЛАГАЕТ НОВЫЙ ВЗГЛЯД НА ФИЗИЧЕСКУЮ ЗАЩИТУ С ПОМОЩЬЮ ВИЗУАЛИЗАЦИИ

Крупчатников Б. Н., консультант ФБУ «НТЦ ЯРБ» (krupchatnikov@secnrs.ru),
Смирнов В. В., канд. техн. наук, старший научный сотрудник (vsmirnov@secnrs.ru)
(ФБУ «НТЦ ЯРБ»)

Введение

Модель угрозы является отправной точкой процесса создания системы физической защиты (СФЗ), она же используется при оценке разрабатываемой и уже созданной на объекте СФЗ. При этом параметры модели угрозы являются гипотетическими, основанными на допущениях о количестве потенциальных нарушителей, их мотивации, вооружении и огневой подготовке, техническом оснащении, тактике действий, осведомленности об объекте, наличии взаимодействия с внутренним нарушителем и пр.

Полномасштабная натурная имитация нападения на ядерный объект имеет очевидные и существенные ограничения, поэтому большое значение придается кабинетным командно-штабным учениям с использованием различных методов симуляции и тренажеров.

Национальная лаборатория Сандия (Sandia National Laboratories) Министерства энергетики США (далее – Лаборатория), которая по их собственной оценке является одной из ведущих организаций в области методологии и технологий физической защиты, разместила информацию на своем сайте (<https://insetools.sandia.gov/>) о программных продуктах нового поколения Scribe3D, CAS Simulator и PathTrace под девизом «новый взгляд на физическую ядерную безопасность посредством визуализации».

Scribe3D

Scribe3D является инструментом для разработки и анализа СФЗ, который позволяет пользователям разыгрывать сценарии атаки и защиты, используя различные высокоточные описания объектов, реквизит, персонал, оружие и транспортные средства. Он может быть использован для создания настольных упражнений, имитирующих кражи, саботаж или стихийные бедствия, позволяет визуализировать атаки и ответные действия в режиме реального времени и показывает реалистичные последствия. Основан на современной технологии игрового движка.

В описании отмечено, что оценка уязвимости СФЗ имеет важное значение для обеспечения готовности организации эксплуатировать объект, а инструменты моделирования и симуляции имеют решающее значение для эффективной, действенной и наглядной оценки и обучения на основе заданных сценариев. С помощью этого инструмента создана серия подробных гипотетических моделей, которые можно использовать для выполнения упражнений, позволяющих оценить и продемонстрировать эффективность систем безопасности и получить результаты для улучшения обучения и модернизации технологий.

Эти базовые модели предназначены для использования на гипотетических объектах, но могут быть адаптированы для разработки и внедрения на объекте пользователя.

Также на сайте указано, что Scribe3D при проведении кабинетных учений с использованием 3D-визуализации позволяет (рис. 1):

- проводить эффективные и наглядные кабинетные упражнения;
- создавать собственные или использовать предварительно разработанные гипотетические модели объектов для тестирования СФЗ, действий сил реагирования и проведения боевых действий;
- оценивать эффективность существующей СФЗ с помощью наглядных настольных упражнений, которые дают научно обоснованные, действенные результаты;
- легко добавлять, перемещать или заменять параметры элементов сил реагирования или элементов технологии для выбора более эффективного варианта;
- вычислять вероятность нейтрализации, используя данные о точности стрельбы и вероятности уничтожения;

- создавать реалистичные сценарии, добавляя более 100 3D-реквизитов, таких как датчики, барьеры, транспортные средства, офисное и вспомогательное оборудование и персонал;
- предлагать или обосновывать модернизацию оборудования перед покупкой каких-либо компонентов;
- разрабатывать сценарии для проверки тактики и процедур сил реагирования и управления чрезвычайными ситуациями;
- создавать видеоролики и записывать результаты из настольных сценариев для разработки последующего обучения персонала службы безопасности и сил реагирования;
- проводить виртуальные экскурсии по объекту и за его пределами для сотрудников регулирующих органов, служб реагирования на чрезвычайные ситуации с использованием гиперреалистичной модели объекта, не нарушая его работу.



Рис. 1. Scribe3D помогает визуализировать атаки и ответные действия в режиме реального времени
 [Fig. 1. Scribe3D can visualize attack and response action in real time]

На сайте Лаборатории представлен демонстрационный видеоролик с одним из сценариев нападения группы из трех вооруженных нарушителей, наглядно показывающий функционал программы и сопровождаемый комментариями о возможностях изменять параметры сценария.

Разработчиками приведено краткое описание следующих гипотетических моделей различных типов ядерных установок и радиационных объектов:

- реактор бассейнового типа (PTR) в институте медицины и физики с ядерными материалами I категории и материаловедческая реакторная установка с ядерными материалами II категории (рис. 2);
- легководный реактор (PWR) (категория: высокие радиологические последствия) (рис. 3);
- малая модульная реакторная установка (SMR) (категория: высокие радиологические последствия), четыре интегрированных реактора SMR, микрореактор – многоуровневое сооружение в сельской местности с реактором с галечным слоем (установка с несколькими зданиями и пунктом контроля входа) (рис. 4);
- транспортный узел – небольшой городской центр с автомобильными, железными дорогами и портом (рис. 5);
- радиационные установки для банка крови (одноэтажное здание, в котором расположены облучатели крови), больницы (многоэтажное здание, в котором находится гамма-нож для телетерапии), панорамного облучателя (объект, где облучение проводится в воздухе в зонах, потенциально доступных для персонала), хранилища (закрытая подземная зона обработки материалов) (рис. 6).

Записи кабинетных учений для анализа и тренировок с применением возможностей Scribe3D Video используются для создания обучающих видеороликов, возможна синхронизация с симулятором CAS для более реалистичного обучения оператора (рис. 7).



Рис. 2. Реакторы бассейнового типа (PTR)
[Fig. 2. Pool type reactors (PTR)]

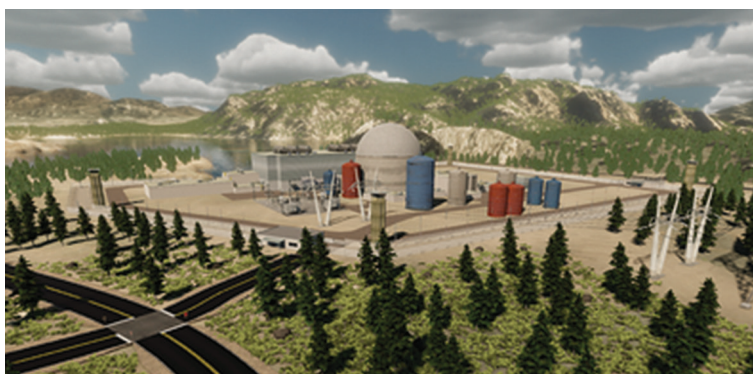


Рис. 3. Легководный реактор (PWR)
[Fig. 3. Pressurized light water reactor (PWR)]

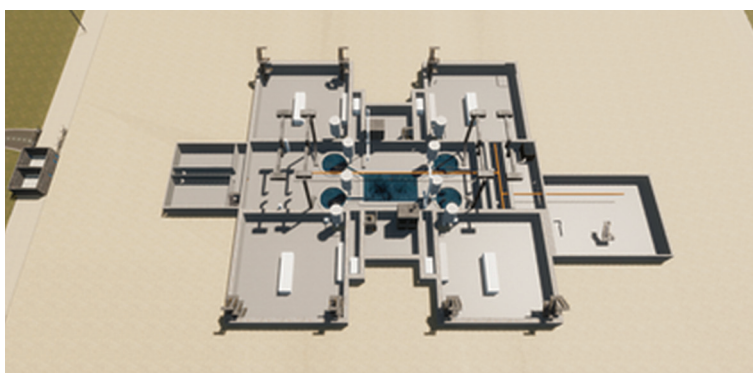


Рис. 4. Усовершенствованные и малые модульные реакторы (SMR)
[Fig. 4. Advanced & small modular reactors (SMR)]



Рис. 5. Транспортный узел
[Fig. 5. Transportation terrain]

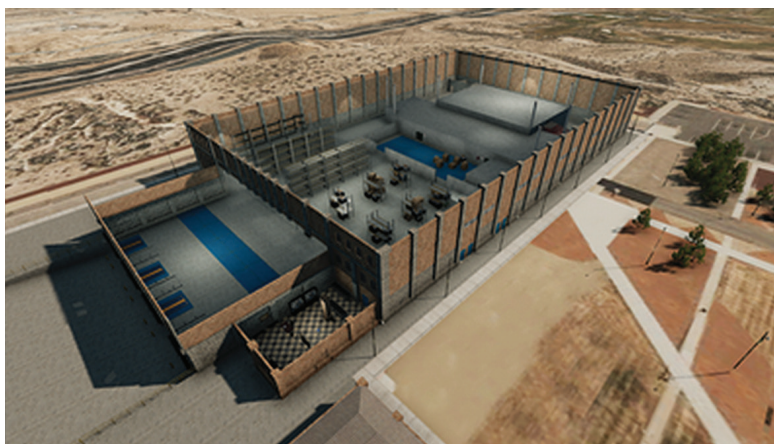


Рис. 6. Радиационные установки
[Fig. 6. Radiological facilities]



Рис. 7. Видеопродукция Scribe3D
[Fig. 7. Scribe3D video production]

CAS Simulator (Central Alarm Station Simulator)

Симулятор центрального пункта управления (CAS Simulator) в СФЗ – комбинированная программно-аппаратная платформа, которая интегрируется практически с любой технологией мониторинга безопасности, для отображения смоделированных сценариев так, как если бы событие действительно происходило на этом объекте (рис. 8, 9).



Рис. 8. Рабочее место симулятора для оператора CAS
[Fig. 8. Simulator workplace for CAS operator]

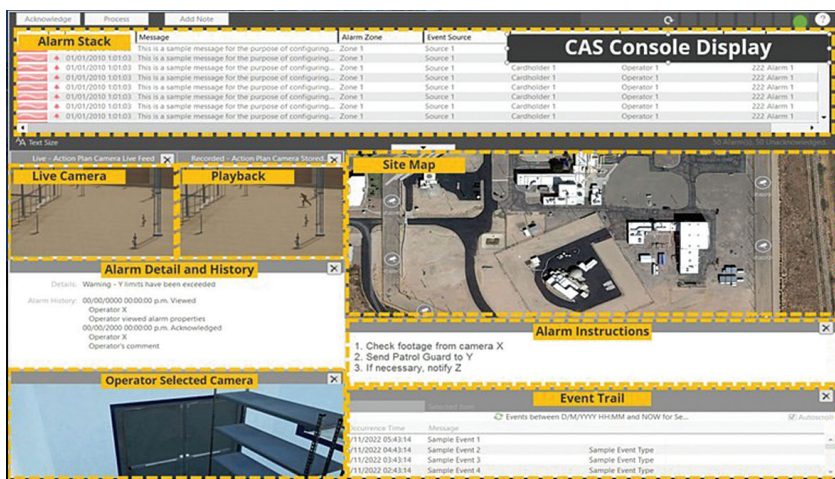


Рис. 9. Пример отображения на дисплее консоли симулятора CAS (на дисплее отображается консоль симулятора – система ввода-вывода данных) [Fig. 9. Illustration of image on the display of the CAS Simulator console]

Отмечаются следующие возможности CAS Simulator для обучения операторов:

- имитация реальной среды, программного обеспечения CAS и сценариев;
- оценка навыков работы операторов CAS и эффективности применяемых на объекте технологий;
- предоставление научно обоснованных данных;
- привлечение операторов CAS, инструкторов, регулирующих органов и руководства для повышения осведомленности о безопасности и улучшения рабочих процедур.

Разработчики подчеркивают, что эффективное обучение требует использования реалистичных сценариев, и отмечают требование к операторам пунктов управления одновременно контролировать множество датчиков и сигналов тревоги, поддерживать связь с силами реагирования и обеспечивать безопасность персонала и материальных ценностей, а также выполнять функции «глаз и ушей» объекта во время чрезвычайной ситуации или нападения. Разработка тренинга для этой сложной и быстро меняющейся задачи является непростым вопросом.

CAS Simulator позволяет устранить проблемы с обучением за счет того, что обеспечивает:

- реалистичность – использование при тренировках реальных и точных данных о технологии безопасности объекта и окружающей обстановки;
- индивидуальные сценарии – применение научно обоснованных данных для устранения как общеизвестных, так и нестандартных угроз;
- ориентированность на результат – представление эффективности работы оператора CAS Simulator в режиме реального времени;
- экономичность – уменьшение затрат, по сравнению с настольными упражнениями или учениями с привлечением сил охраны и имитацией действий нарушителей «в поле»;
- безопасность – проведение обучения, не влияя на текущую безопасность объекта.

На сайте Лаборатории отмечается, что имеются предварительно разработанные сценарии, в частности CAS Simulator предлагает следующие распространенные сценарии обучения: полная атака на объект, несанкционированный доступ и выход из объекта, действия протестующих, потеря связи или кибератака. При этом регулярно разрабатываются новые сценарии.

В скором времени планируется обучение на месте с возможностью:

- смоделировать свой объект или использовать гипотетическую модель;
- создать сценарии специально для каждого предприятия, окружающей обстановки и потребностей в обучении;
- принять участие опытным инструкторам для обучения операторов CAS Simulator со сценариями и проведением обсуждений;
- исключить перерывы в работе объекта или проведение дорогостоящих натурных учений с привлечением сил охраны.

PathTrace

Непрерывная оценка уязвимости системы необходима для обеспечения того, чтобы СФЗ любого объекта функционировала так, как задумано и как требуется. Но перечень средств защиты и технологий безопасности сам по себе не дает представления об эффективности системы, рекомендаций по возможным обновлениям и не позволяет учесть возможности противника.

PathTrace – это инструмент для моделирования и количественного анализа уязвимости объекта, который использует установленные алгоритмы для выявления уязвимостей системы. PathTrace вычисляет вероятность обнаружения нарушителя и вероятность прерывания его действий, определяет критическую точку обнаружения для нескольких путей продвижения и генерирует схему последовательности действий злоумышленников для каждого пути, предоставляя объективно обоснованные данные, что позволяет повысить безопасность на объекте (рис. 10). Данная программа имеет следующие достоинства:

- визуально интуитивно понятный инструмент количественного анализа;
- наличие изображения двухмерного многоэтажного вида объекта;
- возможность простого или сложного анализа траекторий, включающего множество целей, угроз и ответных мер;
- предоставление результатов с использованием научно обоснованных, устоявшихся алгоритмов из апробированных расчетных инструментов.

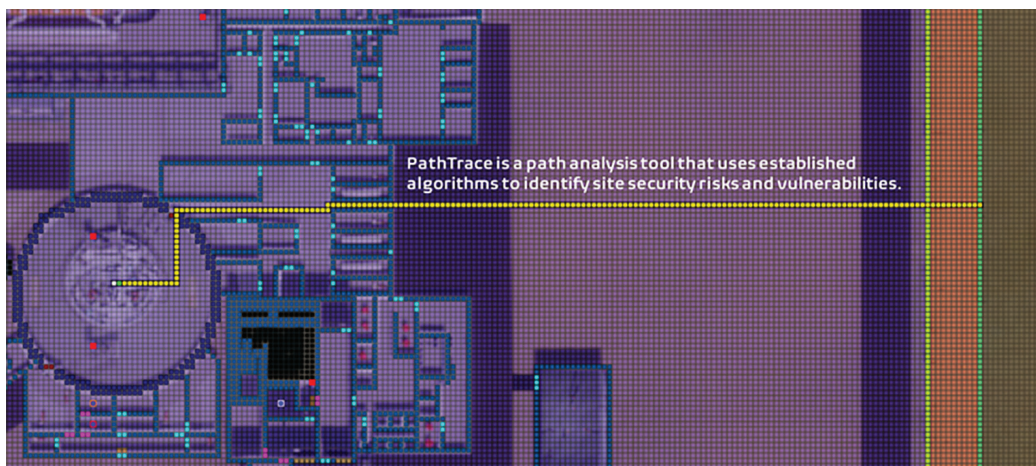


Рис. 10. Пример отображения на дисплее траектории нарушителя на 2D слое модели объекта [Fig. 10. Illustration of displaying the adversary's pass on the 2D layer of the facility model]

Функции PathTrace:

- определяет быстрые и незаметные пути продвижения нарушителя и наиболее уязвимые участки физической защиты на них;
- использует установленные алгоритмы для определения уязвимостей СФЗ;
- вычисляет вероятность обнаружения и прерывания действий нарушителя для нескольких путей его продвижения;
- генерирует критическую точку обнаружения для каждого пути продвижения;
- генерирует диаграмму последовательности действий нарушителя для каждого пути его продвижения;
- позволяет тестировать стратегии смягчения последствий для переменных параметров обнаружения, задержки и реагирования.

Разработчиками даются подробное описание того, как работает PathTrace, и рекомендации по его применению.

Для построения собственной модели объекта (рис. 11) предлагается использовать данные о конфигурации объекта, а именно:

- использовать аэрофотоснимок объекта, взятый из схемы, чертежа, поэтажного плана или даже фрагмента из Google Maps;

- установить барьеры задержки, такие как стены, двери, заборы, ворота и окна, которые остановили бы продвижение атакующего;
- определить области обнаружения, такие как объем контроля датчиков, патрулируемые зоны и охват камер, которые привели бы к обнаружению злоумышленника.

Для определения ответных мер и возможностей противника (рис. 12) необходимо использовать данные о параметрах СФЗ и потенциального нарушителя: необходимо использовать данные тестирования объекта, чтобы указать время реакции группы реагирования на событие обнаружения, а также какие типы инструментов могут быть у противника, и рассмотреть несколько разновидностей наборов инструментов.

Для проведения анализа объекта имеются следующие возможности (рис. 13):

- сгенерировать и оценить самый быстрый, скрытный и наиболее уязвимый путь к цели или набору целей;
- рассмотреть несколько сценариев «что, если»;
- проверить эффективность существующего проекта;
- изучить идеи по модернизации оборудования или технологий, проверить их эффективность и обосновать затраты до того, как они будут внедрены.

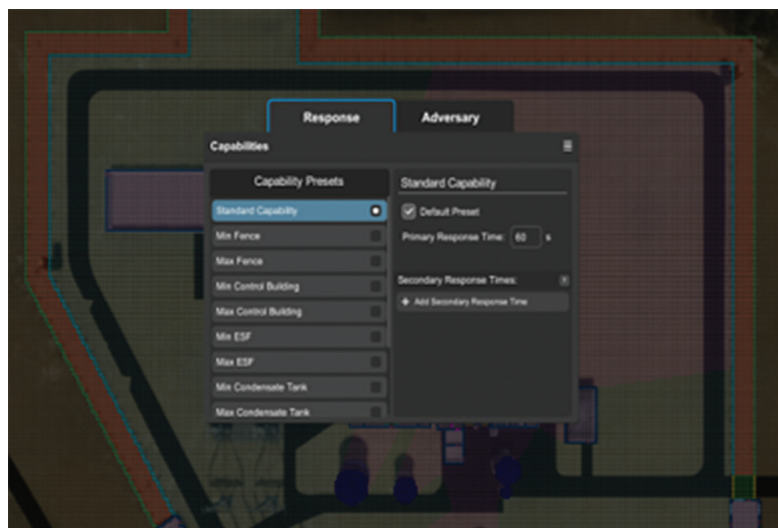


Рис. 11. Построение собственной модели объекта
[Fig. 11. Building your model]

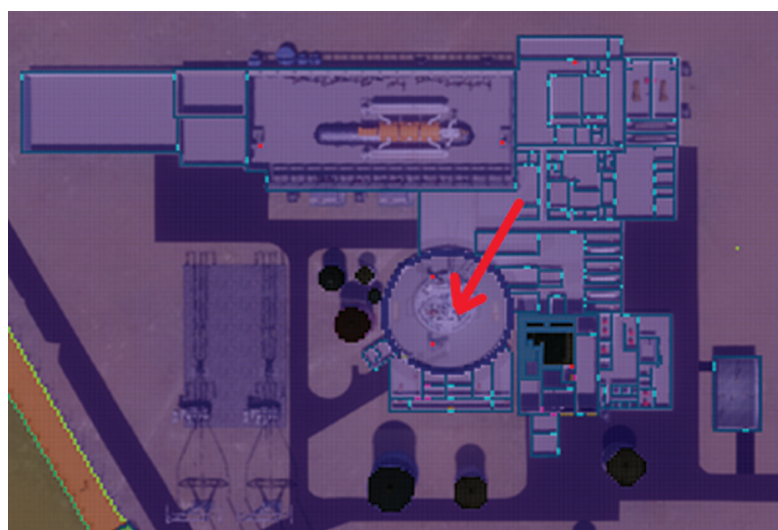


Рис. 12. Определение ответных мер и возможностей противника
[Fig. 12. Defining response and adversary capabilities]

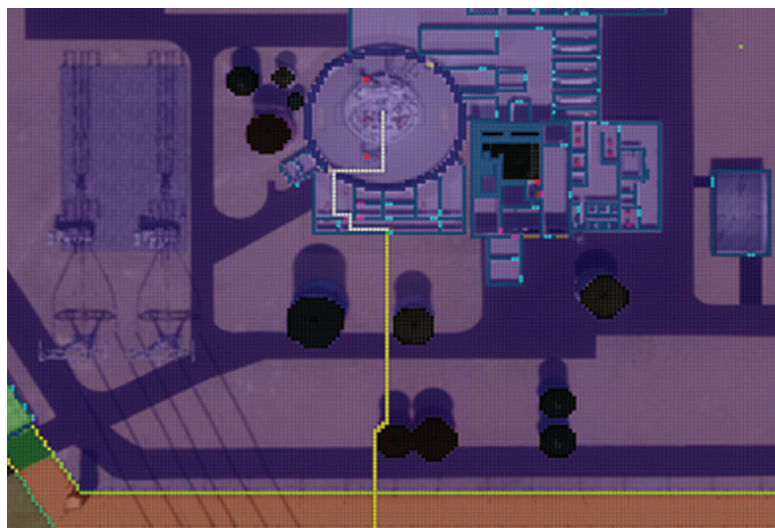


Рис. 13. Проведение анализа объекта
[Fig. 13. Analysis of your facility]

PathTrace предоставляет данные, пригодные для:

- изменения сроков обнаружения, задержки и реагирования с целью повышения уровня безопасности;
- модернизации и тестирования усовершенствованного оборудования перед установкой;
- демонстрации и предоставления данных, подтверждающих эффективность системы;
- обнаружения скрытых путей противника, которые могут быть неочевидны.

Отмечается полезность совместного использования PathTrace и Scribe3D для анализа путей атаки противника и того, как изменения в параметрах обнаружения, задержки или реагирования влияют на безопасность объекта. Последующий экспорт созданной модели в Scribe3D показывает пути атаки противника и ответные действия охраны с целью создания кабинетных учений. Оба инструмента позволяют использовать как количественные, так и качественные методы оценки системы.

Заключение

Представленная на сайте Лаборатории (<https://insetools.sandia.gov>) информация дает достаточно полное представление о возможностях рассмотренных программных средств, одно из которых реализует трехмерную визуализацию (Scribe3D), а другое – двухмерную (PathTrace), и можно отметить, что использование возможностей визуализации процессов в системе физической защиты весьма перспективно.

Предложенные технологии визуализации событий, имитирующих сценарии злоумышленных действий в отношении ядерных и радиационных объектов и возможные ответные действия сил реагирования, в сочетании с симулятором пункта управления в СФЗ, позволяющие адаптировать их к условиям конкретного объекта, являются несомненно полезным инструментом не только для обучения и проверки навыков и профессиональной подготовки персонала физической защиты и сил охраны, но и для проведения оценки эффективности самой СФЗ, выявления и устранения уязвимостей.

Есть основания полагать, что разработчики СФЗ, сотрудники службы безопасности и лица из числа вооруженной охраны, а также их оппоненты – злоумышленники – мыслят примерно одинаково в отношении сценариев возможной диверсии на объекте или хищения ядерных материалов. Таким образом, возможность проигрывать большое число сценариев нападения, а также создавать параметры таких сценариев позволяет сформировать исчерпывающую картину в отношении событий физической безопасности и избежать неожиданного развития событий. При этом результаты такого ситуативного моделирования должны анализироваться, обобщаться и находить отражение в инструкциях и практике ответных действий.

Существенным достоинством описанных инструментов является возможность их адаптации к реальным объектам. При этом, однако, возникает опасение, что такие цифровые аналоги объекта сами будут весьма чувствительной информацией, представляющей большой интерес для потенциальных нарушителей, и нуждаются в исключительно надежных мерах по защите от доступа к этой информации злоумышленников.

Важно отметить, что процесс анализа уязвимости объекта и оценки эффективности СФЗ является наиболее сложным, но и наиболее важным этапом, как при формировании вновь создаваемой СФЗ ядерного объекта, так и при совершенствовании уже существующей системы. Автоматизация этого процесса, создание и совершенствование интерфейса программных комплексов в совокупности с возможностями визуального представления в трехмерном или двухмерном изображении позволит расширить возможности проектировщиков и эксплуатационного персонала, сотрудников иных организаций, участвующих в охране объекта, а также может способствовать лучшей осведомленности специалистов органа регулирования.

Дальнейшее развитие этого направления вполне заслуживает того, чтобы получить распространение среди сообщества специалистов по ядерной физической безопасности, в том числе посредством обмена информацией в рамках инструментов МАГАТЭ.

