УДК:004.942

ИМИТАЦИОННОЕ МОДЕЛИРОВАНИЕ СРЕДСТВ ФИЗИЧЕСКОЙ ЗАЩИТЫНА ОХРАНЯЕМОМ ОБЪЕКТЕ В ЗАДАЧАХ ОЦЕНКИ УЯЗВИМОСТИ

И.К. Шарков (Санкт-Петербург)

Введение

Задача охраны периметра и важных территориальных объектов является фундаментальной с первых моментов появления частной собственности до современных вопросов безопасности. Это справедливо как для гражданских, так и для военных объектов. Хорошо организованная система физической защиты (СФЗ) объекта будет качественно отвечать выставленным к ней требованиям по защищенности и при этом будет лишена избыточности или недостаточности. В зависимости от конкретных целей, которые ставятся при решении задачи безопасности объекта, меняется структура СФЗ и еѐ сложность. При этом, чем сложнее структура такой системы и еѐ внешние условия, тем труднее достоверно оценить еѐ реальное качество по обеспечению безопасности от проникающих угроз с любых направлений при любых внешних и внутренних условиях.

Проблематика создания качественной СФЗ остро стоит в комплексности этой задачи: необходимо обеспечивать правильное использование и условия эксплуатирования всех элементов системы, а так же четко представлять цели и задачи, которые преследует эта система. Чем больше структурных и функциональных элементов в системе, тем сложнее еѐ реакция на воздействие, а неправильно выбранные цели могут частично или полностью нивелировать результат еѐ работы. В данном случае, ТТХ СФЗ любого объекта можно сравнить с вооружением, а если конкретно – с системами ПВО (которые, кстати говоря, могут являться частью такой СФЗ), от правильности организации и актуальности которых зависит уязвимость наземных войск и объектов.

Часто планирование и создание структуры СФЗ осуществляется на основе субъективного взгляда собственника или эксперта по безопасности. При этом особое внимание уделяется формальному соответствию различным требованиям постановлений и норм, но не фактическому соответствию выставленной планке качества. Сама планка качества, как правило, характеризуется несколькими трудно проверяемыми без определенных методик величинами: минимально допустимой вероятностью обнаружения, максимальной периодичностью ложных тревог и т.п. Проверить факт соответствия СФЗ этим параметрам можно различными способами, обладающими своими плюсами и минусами [1]:

- натурные испытания на объекте – проведение множества экспериментов над СФЗ с целью установить примерные значения этих параметров. Эффективный способ проверки, наглядно демонстрирующий результаты. Однако это длительный и, как правило, трудозатратный процесс, позволяющий выборочно оценить части СФЗ, над которыми проводились испытания. При этом система уже должна быть реализована;
- экспертная оценка проекта и его реализации – проверка экспертами по безопасности в сфере СФЗ. Это самый распространенный способ, так как эксперты способны проверить формальное соответствие законам и требованиям, а так же на основе своих знаний и опыта оценить качество реализации проекта и его реализацию. Минусом является субъективность мнения экспертной комиссии, которая может не учесть весь спектр потенциальных уязвимостей и не может проанализировать качество выполнения своей задачи у каждого сегмента системы в условиях объекта;

- компьютерное моделирование – способ оценки фактической защищенности, с помощью которого проводят множество имитационных экспериментов над цифровым двойником СФЗ с целью выявления проектных ошибок и проблем взаимодействия элементов систем друг с другом в динамических условиях внешней среды объекта при акте незаконного вмешательства со стороны выбранной модели нарушителя. Минусом является то, что конечная реализация может отличаться от цифрового двойника СФЗ по качеству монтажа и эксплуатации.

Эффективная комбинация экспертной оценки и использование компьютерного моделирования позволит получить наиболее достоверные результаты о формальном и фактическом качестве СФЗ. Результаты вычислительных экспериментов над цифровым двойником СФЗ позволят повысить объективность экспертного мнения, автоматизировав не только работу по оценке, но с математической точностью учтя все нюансы крупномасштабных систем защиты как гражданских, так и военных объектов. Так на ранних этапах можно составить надежную систему защиты и упредить предотвратить неоправданные финансовые затраты. Так же, для уже построенных систем можно выявлять неочевидные факты несоответствия требованиям физической безопасности из проекта и разрабатывать возможные решения, по исправлению обнаруженных уязвимостей.

Имитационное моделирование жизнедеятельности цифровых двойников СФЗ объекта помогает определиться со стратегией защиты на разных участках СФЗ и степенью эффективности этих стратегий в противодействии тем или иным угрозам. В практике часто упоминаются такие программные комплексы как ВЕГА-2 (СНПО «Элерон»), Итерация (АО «Итерация», Россия), САПР СИТЗО «Амулет» (АО Производственно-внедренческое предприятие «Амулет», Россия), EASI (Estimate of Adversary Sequence Interruction), ASSESS (Analitic Systemand Soft ware fo Evaluating Safeguards and Security) («Сандийские национальные лаборатории», США), СПРУТ (НПП «ИСТА-Системс», Россия). Задача этих комплексов – анализ СФЗ и оценка еѐ эффективности. При этом каждый из программных комплексов использует различные подходы, однако, большинство из которых сводится к гонке по времени нарушителя и сил службы безопасности. Лишь некоторые из перечисленных программных комплексов обращаются в процессе анализа к имитационному моделированию, однако при этом происходит моделирование не всей СФЗ, а отдельных еѐ элементов и процессов [2]. Например, боестолкновение «нарушитель-охранник» или обнаружение нарушителя методом точечных статистических испытаний.

Таким образом, имитационного моделирования всей системы в формате крупномасштабной модели не проводится. Чаще всего сам процесс сводится к исследованию жестко заданных сценариев, на основе которых разыгрывается вероятностно-временной подход к оценке эффективности СФЗ [3]. Такой процесс анализа можно назвать достаточно точным для конкретных участков системы, но нельзя достоверно оценить проектируемую СФЗ в целом.

В данном материале рассмотрен подход к моделированию СФЗ объекта для разнообразных и реалистичных имитационных экспериментов с проникновением на территорию цифрового двойника объекта выбранной модели нарушителя с целью получения точных оценок характеристик защищенности. Математические модели всех структурных элементов СФЗ, нарушителя и внешних условий составлялись с помощью отечественного программного обеспечения Rand Model Designer на объектно-ориентированном языке моделирования высокого уровня, основанный на объектной парадигме UML, позволяющий быстро и качественно создавать сложные модели [4]. Такой подход позволит промоделировать всю исследуемую систему со всеми параллельными процессами, соответствующими как инженерно-технической системам

охраны, так и сотрудникам службы безопасности, внешним условиям и нарушителю. В отличие от большинства других подобных проектов, данная разработка не закрыта под грифом ДСП и позволяет сторонним специалистам оценить логические схемы моделей и их взаимосвязей за счет читаемого и понятного стандарта UML.

Поставленная цель

Существует потребность в создании комплексного решения формирования математических моделей цифровых двойников СФЗ для формирования объективной оценки качества будущей или существующей системы на основе проведения множества имитационных экспериментов с актом незаконного вмешательства различных моделей нарушителя. Целью работы стало исследование возможности создания с помощью языков объектно-ориентированного моделирования работоспособной комплексной математической модели СФЗ для формирования таких цифровых двойников и проведения имитационных экспериментов с проникновением.

Выбор программного средства

Имитационная модель СФЗ должна быть целостной динамической системой, моделируемой не только по времени функционирования, но в геометрическом пространстве (траектории движения, геометрия препятствий и т.д.) [5]. Для полноценного моделирования подобной системы необходимо применять современные инструменты математического моделирования, такие как MATLAB, Dymola или Rand Model Designer [6] (RMD). Модели, созданные с помощью таких инструментов, могут в перспективе использоваться программными средствами, специализирующимися на проектировании и моделировании СФЗ охраняемых объектов. Похожий опыт применения моделей из пакетов компьютерного моделирования хорошо опробован в системе имитационного моделирования RMD [7], которая позволяет создавать встраиваемую имитационную модель в виде динамической библиотеки Windows (DLL). Кроме того, RMD является отечественным программным продуктом, что значительно снижает его стоимость при коммерческом использовании в сравнении с конкурентами, не ограничивая функциональность.

Пакет RMD использует декларированный объектно-ориентированный язык моделирования высокого уровня Modelica, основанный на объектной парадигме UML, позволяющий создавать модели крупномасштабных систем [8]. При этом RMD является единственным универсальным инструментом, позволяющим создавать все виды моделей динамических систем, что дает возможность разрабатывать модели, включающие в себя категорично разные элементы систем (человек-охранник, датчик, погода, ложные тревоги и т.д.). При моделировании полноценной СФЗ в RMD доступна разработка непрерывных, дискретных и гибридных (непрерывно-дискретные) моделей, применимых для каждого из элементов системы, и проведение с ними интерактивных вычислительных экспериментов в едином вычислительном эксперименте [8].

При этом, существует возможность изменения и редактирования логик моделей без значительного изменения использующего их программного обеспечения – возможность использования описанного интерфейса взаимодействия с разработанными динамическими моделями математических моделей. Это крайне важно, когда речь идет о новых требованиях к охране объектов, появлении новых элементов системы защиты (видеокамер, извещателей), о появлении угроз, которые ранее не принимались в расчет или не были до конца изучены.

Теоретическая и постановочная часть

Для разработки имитационной модели СФЗ был выбран Rand Mode lDesigner 7, который подходил для выполнения задачи. Также необходимо было определить, какие

структурные элементы СФЗ будут смоделированы. Они стали основой базовых математических моделей, используемых для создания имитационной модели.

Такая имитационная модель должна включать в себя как минимум четыре параллельных процесса, независимо развивающихся в модельном времени и взаимодействующих между собой [9]:

- моделирование действий нарушителя;
- моделирование работы инженерно-технических средств охраны (ИТСО);
- модель действий оператора;
- модель действий группы реагирования.

Для каждого элемента, используемого в имитационной модели и обладающего собственной функциональностью (например, извещатель с переходным процессом выработки сигнала тревоги), запускается свой независимый процесс.

Список моделируемых элементов в настоящий момент представляет собой UML-модели с гибкими параметрическими настройками:

- нарушитель – человек, совершающий акт незаконного вмешательства на охраняемую территорию объекта. С помощью параметров задаются различные модели поведения нарушителей: от дилетанта до диверсанта или террориста;
- специфическая область – зона движения, обладающая специфическими свойствами видимости и проходимости. Например: болото, асфальтированная дорожка, кустарник;
- препятствие – инженерное средство охраны, замедляющее проникновение нарушителей по периметру или его участку. Препятствием может быть ограждение, барьер, шлагбаум, ров и т.д. в зависимости от параметров;
- ворота – часть ограждения, позволяющая осуществлять санкционированный проход для сотрудников службы безопасности через ограждение;
- охранный извещатель – датчик, обладающий обнаруживающей способностью. Описаны основные виды охранных извещателей;
- охранная видеокамера (CCTV) – устройство для дистанционного наблюдения за заданной территорией объекта. Описаны стационарные и поворотные видеокамеры;
- видеоаналитика – технология, использующие методы компьютерного зрения для автоматизированного обнаружения с помощью CCTV нарушений границ охраняемой территории;
- оператор службы безопасности (ОпСБ) – оператор, отвечающий за принятие решений на охраняемом объекте: наличие и отсутствие тревоги, контроль ложных тревог, координация действий сил службы безопасности;
- оператор системы видеонаблюдения (ОпСВН) – оператор, отвечающий за обзор доступных видеокамер, визуальное обнаружение и сопровождение нарушителей;
- группа реагирования – группа сотрудников службы безопасности (охранник), которая выполняет задачи по перехвату и нейтрализации обнаруженного нарушителя;
- погодные условия – метеорологические условия, влияющие на дистанцию видимости, обнаруживающую способность извещателей и возникновение ложных тревог;
- ложные тревоги – сигналы тревожного извещения с датчиков системы, которые могут возникать вследствие ошибки оборудования, влияния погодных условий или саботажа.

Количественный состав, локальная/частная логика работы, параметры, взаимодействие с системой и взаимное расположение всех элементов описываются входными данными. Из них создается будущая математическая модель охраняемого объекта. После модель СФЗ проверяется с помощью собственных возможностей RMD (инструмент «визуальная модель») без использования каких-либо сторонних

программных средств, но в которые создаваемые модели могут быть встроены в перспективе.

Для имитационной модели СФЗ необходимо было ввести понятие «план объекта» – это карта охраняемого объекта, составленная из моделируемых элементов (строения, препятствия, нюансы окружающей среды и прочее). В качестве «плана объекта» использовался текстовый файл, в котором записаны все наименования, геометрические формы и координаты моделируемых элементов. Это удовлетворяло условию того, что для моделирования в RMD вся структура СФЗ должна быть описана входными параметрическими данными. При этом не все модели требуют геометрические описания или координаты (например, погодные условия).

Создавать «план объекта» можно с помощи различных графических редакторов и программ (например, AutoCAD, КОМПАС и т.д.), добавляя каждой геометрической фигуре свойства. В данном исследовании карты были построены при помощи программного комплекса «АКИМ» компаний ООО «Комплексные системы» и ООО «Пентакон».

Результаты

В ходе разработки средствами RMD была получена математическая модель СФЗ, в состав которой вошли такие моделируемые элементы, как инженерные и технические средства охраны, специфические зоны, так нарушитель и охранник. Кроме того, над всем этим существуют модели погоды, оператора СБ и СВН, модель ложных тревог и т.д.

Если создать простую СФЗ, то моделируемая система может выглядеть как на примере рисунок 1, где изображен необходимый минимум для демонстрации работы. Такой план можно собрать в редакторе цифровых двойников объектов из специально разработанного программного комплекса экспертного моделирования «АКИМ». Здесь существуют как инженерные и технические средства охраны, специфические зоны, так нарушитель и охранник. Кроме того, над всем этим существуют модели погоды, оператора СБ и СВН, модель ложных тревог и т.д.

Каждый из моделируемых элементов имеет свои собственные карты поведения (логики) с наличием различных состояний, управляемых внутренними параметрами. У элементов есть как внутренние, так и внешние связи, необходимые для внутренней логики и для взаимодействия со внешней моделируемой средой. Так, например, у извещателя есть множество модельных параметров, отвечающих за обнаруживающую способность (вероятность), задержки сигналов, минимальные/максимальные допустимые характеристики условий обнаружения, параметры геометрической формы (зоны обнаружения и положения устройства датчика в пространстве) и так далее.

Примеры нескольких карт поведения различных классов моделируемых элементов СФЗ представлены на рисунке 2. Представлены нарушитель, ложные тревоги, извещатель и оператор СБ. Поподробнее со структурой моделей можно ознакомиться в других публикациях автор [9, 10].

Для проверки модели и проведения экспериментов с проникновением нарушителя в RMD необходимо запустить инструмент «Визуальная модель», которая создаст класс модели vmModel. В этот класс будут включены все упомянутые "планом объекта" моделируемые элементы и задано их относительное друг друга положение в пространстве.

Рис.1 – План простой СФЗ в редакторе «АКИМ»

Для того, чтобы сообщить RMD входные данные из "плана" для моделирования, эту информацию следует передать в текстовом представлении с использованием специального расширения языка XML.

Модель СФЗ включает в себя определения классов, типов, глобальных констант, параметров и переменных, а также глобальных процедур и функций. Используются элементы импортируемых пакетов Statistics, List, System. Диаграмму организации и наследования классов моделей можно увидеть на рисунке 3.

Начальная информация, необходимая для имитационного моделирования, содержит описание сгенерированной траектории нарушителя/охранника, описание элементов инженерных и технических средств охраны (ограждений, камер и т.п.), описание параметров модели, описание параметров оператора СБ, операторов СВН, погодных условий, групп реагирования и патрулей. Каждому моделируемому элементу СФЗ назначается уникальный идентификатор – целое число, играющий роль ссылки на соответствующий элемент на "плане объекта".

Сгенерированная траектория нарушителя/охранников разбивается на последовательность фрагментов. Фрагментам соответствует равномерное прямолинейное движение, а в точках пересечения фрагментов траектории с другими элементами «плана» соответствуют качественные изменения – переход на другой участок ломаной, вход в зону извещателя/камеры, выход из зоны извещателя/камеры, начало преодоления препятствия, окончание преодоления препятствия и т.п.

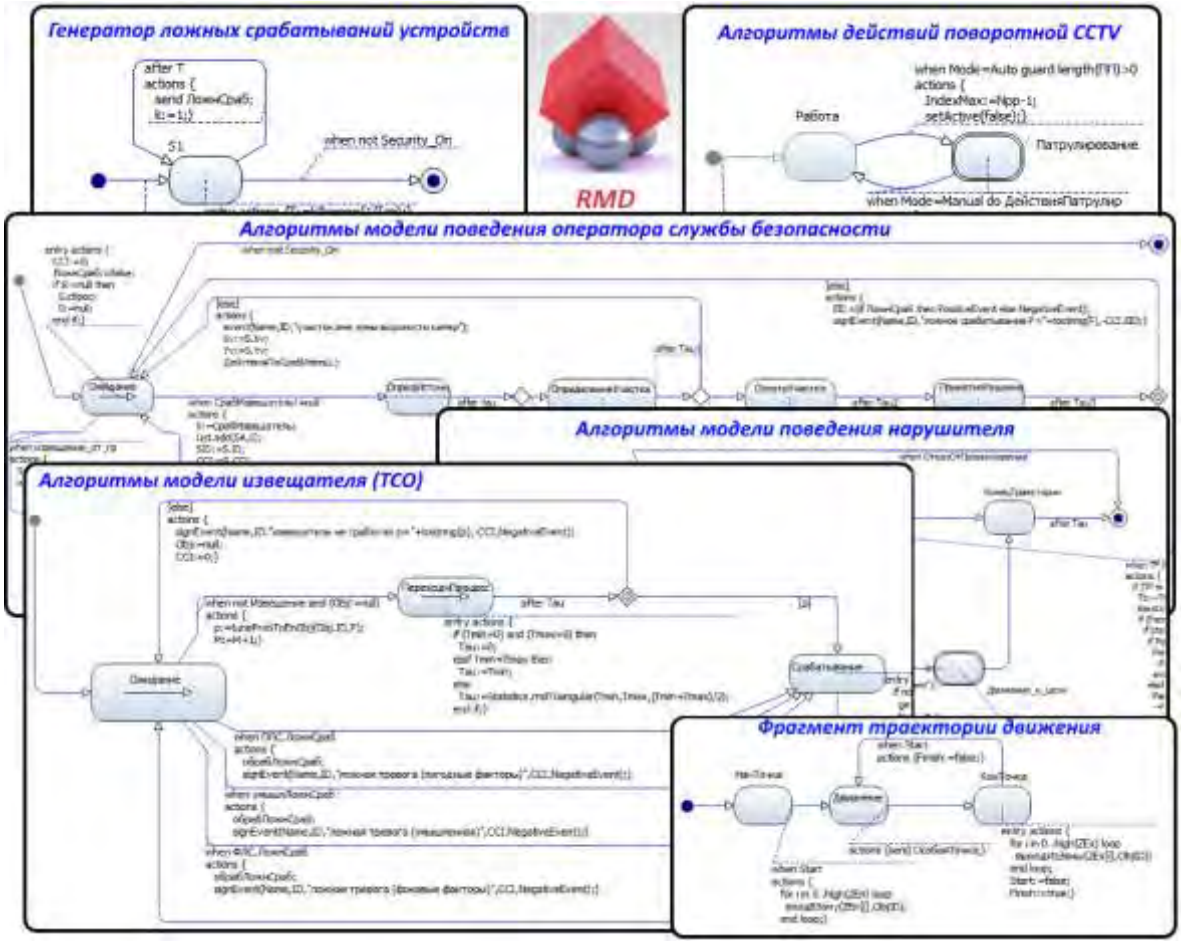

Рис.2 – Карты поведения различных моделируемых элементов в RMD 7

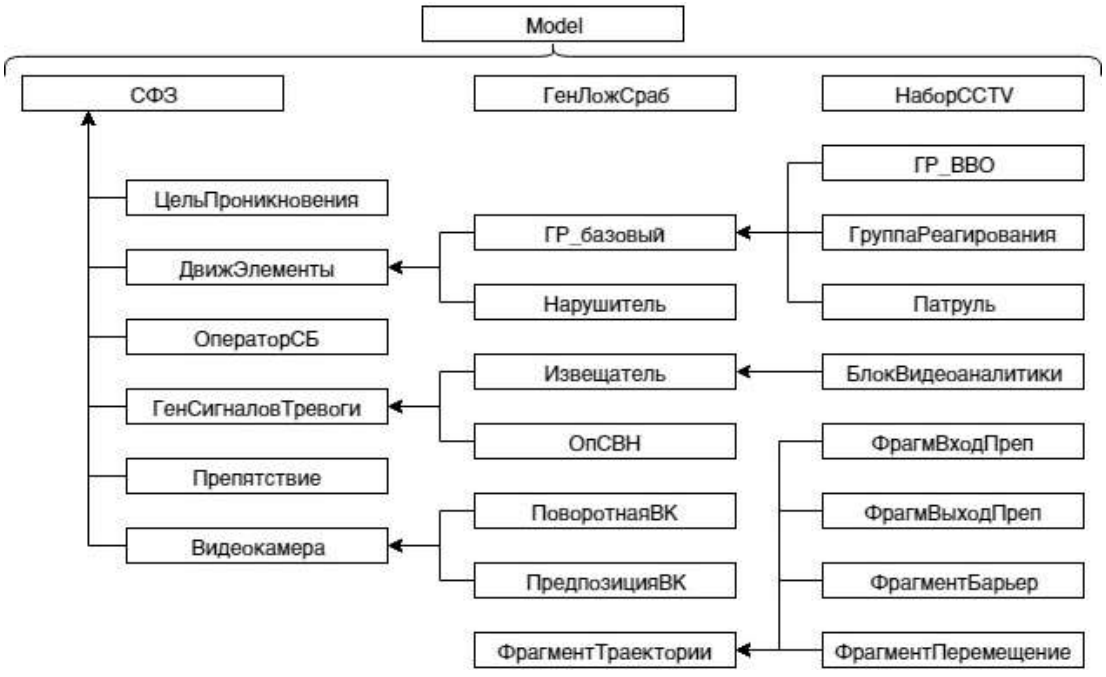

Рис.3 – Структура классов моделей элементов СФЗ, нарушителя и т.д.

Предварительное определение точек событий (изменений условий) позволяет существенно повысить скорость и точность моделирования. Альтернативный подход, предполагающий определение точек изменений в процессе моделирования (например, входа в зону извещателя или преодоление ограждения), требует существенных вычислительных затрат и чреват пропуском точек изменений.

В ходе моделирования модель СФЗ может запрашивать дополнительную информацию (например, изменение траектории движения) с помощью «обратного вызова» доступной в профессиональной версии RMD.

Для работы математической модели в сторонних приложениях необходимо создать программную оболочку, которая позволит подключаться к экспортированной динамической библиотеке модели. Запускающая программа должна создавать экземпляр класса модели, указав путь к файлу dll, и далее вызывать методы этого объекта. Класс модели в программе будет наследоваться от класса vmModel, используемого внутри RMD [10].

Для каждого испытания приложение должно создать новый экземпляр класса модели и с его помощью осуществлять соответствующий эксперимент над моделью СФЗ (при повторных вызовах конструктора используется уже имеющаяся ссылка на загруженную операционной системой dll математической модели).

Перед запуском моделирования СФЗ приложение должно передать в модель информацию о «плане объекта», содержащую уникальные условия. Дело в том, что большое количество моделируемых элементов имеют параметры вероятности возникновения того или иного события. Технические средства охраны обладают заданной вероятностью обнаружения и временем наработки на ложную тревогу (можно взять из технической документации устройств). Операторы службы безопасности обладают вероятностью принятия правильного решения. Кроме того в модели случайным образом для каждого эксперимента из заданных диапазонов определяются скорости движения на фрагментах траекторий, задержки сигналов, время преодоления препятствий и так далее.

Таким образом, каждый эксперимент с проникновением при имитационном моделировании цифрового двойника объекта обладает уникальными и практически неповторимыми (зависит от степени сложности системы) событиями и условиями проведения.

Пример работы модели

Для демонстрации работы созданной имитационной модели опишем ход одного эксперимента, который был воспроизведен с помощью созданной программной оболочки.

Был построен небольшой проект СФЗ охраняемого объекта, на территории которого размешены следующие элементы: два ограждения, система видеонаблюдения, извещатели, здания, группа реагирования (далее ГР) и траектории движения для нарушителя и ГР. Траектории заданы сразу целиком от старта до финиша, но в процессе имитационного моделирования такие траектории были бы созданы фрагментами с множеством различных точек старта за пределами объекта с помощью отдельного прокладчика «Polaris» [5]. К прокладчику моделирующая программа должна обращаться при каждом событии изменения траектории. В демонстрационном примере траектории не являются динамическими.

Система была создана таким образом, чтобы в ней были уязвимые части. Схематическое изображение описанной СФЗ объекта представлено на рисунке 4.

Каждому из моделируемых элементов были заданы конкретные параметры, определяющие поведение данного элемента в процессе моделирования. На основе

схематического изображения (рисунок 4) в программном комплексе «АКИМ» был создан «план объекта», представленный на рисунке 5.

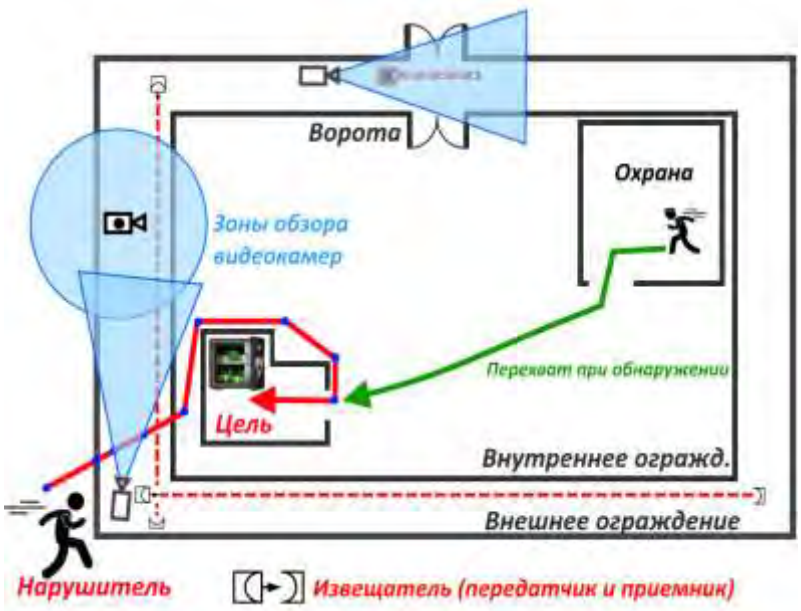

Рис.4 – Изображение СФЗ

Моделирование проводилось как по заданным траекториям нарушителя, так и по генерируемым прокладчиком Polaris [5]. В зависимости от траектории и разыгранных случайных величин (скорость движения, время задержки на препятствии, вероятность срабатывания датчика и т.п.) получался один из двух результатов: пропуск или успешный перехват. Собирая статистику результатов экспериментов по множеству траекторий, направленных к заданной цели проникновения, можно получить соотношение пропусков к успешным перехватам. Ограничить объем выборки удается с помощью заданного доверительного интервала [11, 12].

Рис.5 – «План объекта» СФЗ в редакторе «АКИМ»

Полученные данные в ходе экспериментов позволяют сформировать ряд характеристик, описывающих качество ТТХ СФЗ охраняемого объекта, например: вероятность успешной нейтрализации нарушителя на конкретном участке, вероятность обнаружения проникновения с помощью ТСО, среднее время задержки нарушителя на ИСО и так далее. Примеры цифровых двойников объектов и процесс моделирования с

результатами показаны на рисунке 6. Так же результаты сохраняются в текстовые протоколы имитационного моделирования, из которых формируются программные отчеты для оператора.

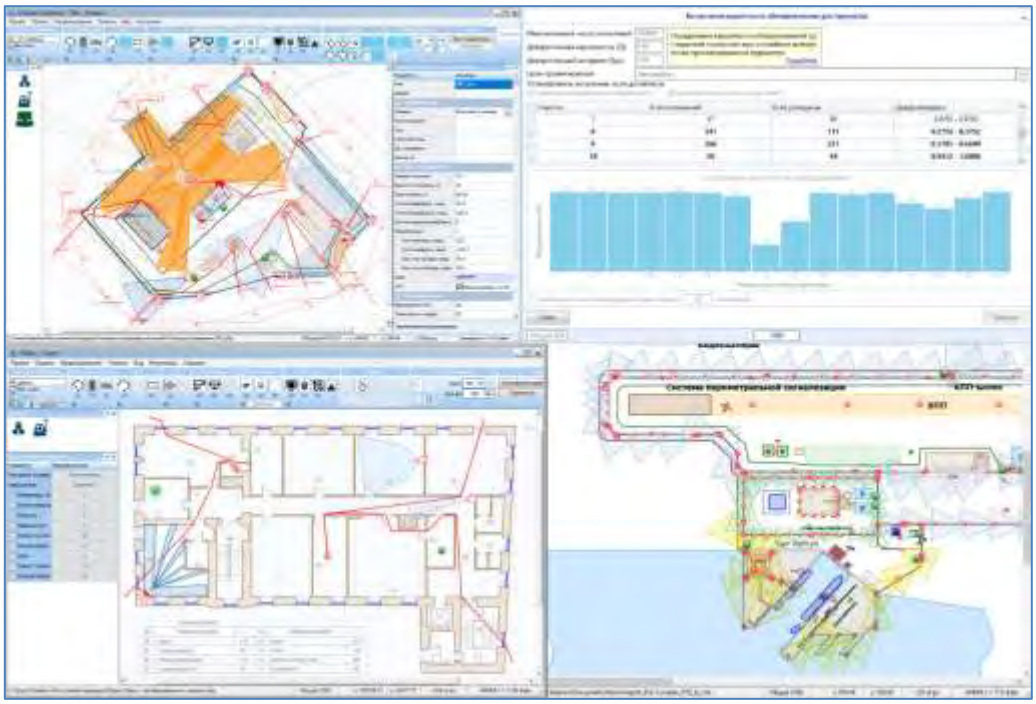

Рис.6 – Примеры цифровых двойников объектов и полученных результатов в «АКИМ»

Выводы

В результате проведенного исследования была изучена возможность применения средств объектно-ориентированного моделирования в задачах оценки уязвимости охраняемого объекта. При помощи среды разработки имитационных моделей RMD была создана математическая модель СФЗ, в которой были описаны её основные структурные элементы, определены их параметры и влияние элементов друг на друга в процессе моделирования. Полученная комплексная математическая модель является основой для создания имитационной модели СФЗ в среде RMD или любом адаптированном для взаимодействия с dll модели программном средстве. С помощью этой модели можно проанализировать спроектированную СФЗ, которая будет описана требуемыми входными данными.

Таким образом, становится возможным проведение анализа эффективности СФЗ путем вычислительных экспериментов, где все моделируемые элементы будут существовать в единой системе.

Было выяснено, что при проведении серий экспериментов с различными конфигурациями СФЗ можно определить наиболее оптимальную структуру защиты той или иной цели. Полученная статистика позволяла вывести оценку эффективности защиты как на пути отдельной траектории, так и для всего плана СФЗ в целом.

Благодарности

Выражаю благодарность за помощь в создании математической модели и консультировании по работе с RMD 7 Колесову Юрию Борисовичу и Инихову Дмитрию Борисовичу, за научную и академическую поддержку Сениченкову Юрию Борисовиу. Хочу поблагодарить коллег в компании «ПЕНТАКОН» Крылова Виктора

Михайловича и Квачадзе Василия Роландовича за помощь в формировании целей и задач создаваемых моделей.

Литература

1. **Шанаев Г.Ф., Леус А.В.** Системы защиты периметра. – М.: Секьюрити Фокус, 2011. – 280 с.
2. **Тарасов А.Д.** Метод и алгоритмы проектирования систем физической защиты объектов информатизации на основе обработки нечеткой информации: дис. на соиск. учен. степ. канд. тех. наук: 05.13.19: защищена 15.12.17 / Тарасов Андрей Дмитриевич. – Уфа, 2017. – 144 с.
3. **Степанов Б.П., Годовых А.В.** Основы проектирования систем физической защиты ядерных объектов: учебное пособие / Томский политехнический университет. – Томск: Изд-воТомского политехнического университета, 2009. – 118 с.
4. **Якимов И.М., Кирпичников А.П., Халиуллин Р.Ф., Мальцев С.А., Ситдиков М.Ш.** Имитационное моделирование в системе Rand Model Designer/ Вестник технологического университета, 2017, Т.20, №2. – 4 с.
5. **Шарков И.К., Желудков Е.А.** Генерация траекторий для задач моделирования СФЗ – Сборник МСИТ 2018 / Томский политехнический университет. – Томск: Изд-во Томского политехнического университета, 2019. – 514 с.
6. **Колесов Ю.Б., Сениченков Ю.Б.** Объектно-ориентированное моделирование в среде Rand Model Designer 7: Изд. Проспект, 2016. – 256 с.
7. **Tarasov S.V.** Application experience of component modeling in Transas Group’s training system development for cargo-ballast and process operations / Tarasov, S.V. Autom Remote Control (2016) 77: 1106. https://doi.org/10.1134/S0005117916060151.
8. **Колесов Ю.Б., Сениченков Ю.Б.** Математическое моделирование гибридных динамических систем.СПб.: Изд-во СПбГПУ, 2014. – 236 с.
9. **Шарков И.К.** Презентация доклада: Применение ООМ при создании моделей систем защиты периметра // КОМОД-2017. URL: http://www.mvstudium.com/ downloads/safe(sharkov)2017.pdf (дата обращения: 01.10.2018).
10. **Шарков И.К.** Применение ООМ при создании моделей систем защиты периметра. // КОМОД-2017. URL: http://dcn.icc.spbstu.ru/index.php?id=377&L=2%252527%2522 (дата обращения: 01.10.2018).
11. **Рыкунов В.Д.** Охранные системы и технические средства физической защиты объектов. – Москва: Секьюрити Фокус. – 2011. – 287 с.: ил. – (Серия "Энциклопедия безопасности").
12. **Гмурман В.Е.** Теория вероятностей и математическая статистика: Учебное пособие для вузов. – 9-е изд. – М.: Высшая школа, 2003. – 479 с.