УДК:004.942

ГЕНЕРАЦИЯ СЦЕНАРИЕВ АТАК НАРУШИТЕЛЯ С ПОМОЩЬЮ АЛГОРИТМА СОБЫТИЙНО-УПРАВЛЯЕМЫХ ТРАЕКТОРИЙ

В.М. Крылов, И.К. Шарков (Санкт-Петербург)

Введение

Важной задачей для всех объектов повышенной важности (от аэропортов до объектов топливно-энергетического комплекса) является обеспечение физической безопасности на их территории от проникновения или негативного воздействия внешних нарушителей. Для этого используются Системы Физической Защиты (СФЗ) – комплекс инженерно-технических и человеческих мер по обеспечению физической безопасности от различных видов угроз. Степень эффективности работы такой системы определяется различными критериями безопасности, такими как вероятность обнаружения нарушителя, вероятность нейтрализации и так далее.

Существуют различные методологии определения эффективности работы системы защиты охраняемого объекта. Одной из методологий является проведение вычислительных экспериментов с помощью имитационного моделирования. Она активно используется в задачах количественной оценки качества защищенности СФЗ охраняемых объектов. Такая оценка важна для понимания сильных и слабых сторон защиты, а это, в свою очередь, помогает принять более обоснованные решения по изменению системы для повышения еѐ эффективности.

Для получения оценок качества СФЗ используются результаты имитационных экспериментов над цифровым двойником СФЗ (в различных представлениях) с выбранными моделями угроз, воздействующими на неѐ. Одной из самых важных частей таких экспериментов, которая влияет на результаты, является создание сценария проникновения внешней угрозы.

Существуют различные методы создания сценариев для вычислительных экспериментов с проникающими угрозами на территорию охраняемого объекта [1]. Наиболее приближенными к реальности являются сценарии, в которых планируется физическое проникновение некоторого нарушителя (например, человека или БПЛА-нарушителя) по некой траектории через структуру СФЗ. Такое проникновение должно быть способно оказывать воздействие на систему защиты, вызывая еѐ ответную реакцию. Реакция СФЗ на такое воздействие является частью этого сценария и может определенным образом влиять на ход событий. Однако не во всех существующих подходах сценарии являются динамически изменяемыми или не ограничены малым числом вариантов развития событий.

Существующие подходы формирования сценариев проникновения.

В практике существует несколько основных хорошо известных и используемых подходов в создании (генерации) сценариев в моделировании проникновения:

№ 1. Предопределенные сценарии проникновения – это сценарии, в которых заранее определены все события по ходу моделирования с их параметрическими величинами (вероятность обнаружения датчиками на определенных точках пути проникновения, время реакции и прибытия охранников, время задержки нарушителя на инженерных средствах охраны и т.д.). Примерами являются программы EASI, ASSESS, SAVI (МАГАТЭ) [2] и т.п.

№ 2. Сценарии проникновения на основе графов. Такие сценарии формируются с помощью создания вариантов путей на заданном графе различными алгоритмами: от

алгоритмов поиска кратчайшего пути [3] до генетических алгоритмов [4]. Примерами являются «ВЕГА-2» (Элерон), «Модель СФЗ» (Итерация).

№ 3. Точечные сценарии на основе случайных воздействий. Это сценарии, получаемые при моделировании случайных воздействий в контролируемом объеме в соответствии с методом Монте-Карло [5], представляющим собой воспроизведение большого числа реализаций случайного процесса, специально построенного по условиям задачи. Такие сценарии дают результаты расчетов для каждой отдельной точки на территории охраняемого объекта за счет расчета заданных формул в области. Примером является «САПР СИТЗО» (Амулет).

В задачах оценки качества СФЗ каждый из данных подходов формирования сценариев накладывает свои ограничивающие условия по реализации. Это влияет на специфику результатов оценки качества СФЗ, их уровень абстракции и скорость их получения. Таким образом, важно четко определять цели и требования для задач анализа уязвимости СФЗ, чтобы выбрать подходящий способ формирования сценариев для вычислительных экспериментов. Из всех трех выделяется № 3, который можно исключить из-за специфики испытаний – сценарий предполагает, что нарушитель появляется в какой-то точке, и для неѐ происходит расчет «обнаружения»/«пропуска». Он подходи для проверки обнаруживающей способности СФЗ по площади объекта.

Общей чертой сценариев атак на СФЗ в подходах № 1 и № 2 является путь проникновения нарушителя и ответная реакция системы. Пример развертки одного сценария можно увидеть на рисунке 1.

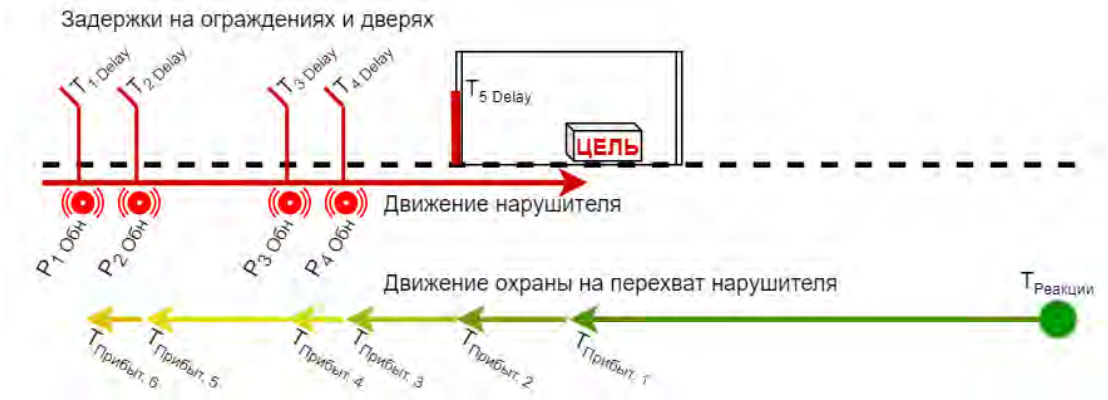

Рис. 1 – Развертка сценария в виде последовательности событий с расчетом времени прибытия охраны на место сигнала тревоги

На рисунке 1 рассматриваются такие параметры и события сценария как:

$\mathbf{T_{i\ Delay}}$ – время преодоления препятствия нарушителем (ограждения, двери, шлагбаумы и т.д.);

$\mathbf{T_{Реакции}}$ – время реакции службы безопасности на сигналы тревоги;

$\mathbf{T_{Прибытия\ j}}$ – время прибытия охраны на то или иное место тревоги для перехвата нарушителя. Чем дольше время движения, тем менее вероятен перехват нарушителя;

$\mathbf{P_{n\ Обн}}$ – вероятность обнаружения нарушителя с помощью технических средств охраны, встреченных на его пути движения.

Формированием сценариев для подходов № 1 и № 2 занимается специально подготовленный специалист в области анализа угроз СФЗ (например, сотрудник экспертной организации). Он определяет ряд параметров и условий для каждой ключевой точки формируемого сценария, выбирает количество и последовательность

этих ключевых точек, локальные оценки качества для критических элементов СФЗ [4]. Сценарий в первом приближении для такого специалиста – путь движения нарушителя извне объекта через его СФЗ к указанной цели. Данный путь характеризуется событиями в ключевых точках (КТ) и характером траекторией движения (не всегда, если система описывается последовательно – это могут быть табличные данные как в EASI).

Каждое событие в КТ представляет собой проверку вероятности какой-либо реакции со стороны СФЗ. Например, срабатывание охранного извещателя и вероятность правильной обработки сигнала на посту охраны. Все вероятностные события (вероятность обнаружения техническими устройствами $\mathbf{P_{Обн}}$, вероятность правильной обработки сигнала $\mathbf{P_{Обр}}$ и т.д.) и другие возможные параметры в каждой встреченной нарушителем КТ участвуют в расчете реакций охранной системы – вероятности поднятия тревоги (см. рисунок 2) [6]. Вероятностное событие поднятие тревоги в свою очередь влечет сценарный расчет вероятности нейтрализации ($\mathbf{P_{Нейтр}}$). $P_{Нейтр}$ может быть рассчитана как формульным путѐм (1), так и являться результатом ответного сценария реакции системы, представляемого аналогичным образом, как и описанный ранее сценарий проникновения по КТ.

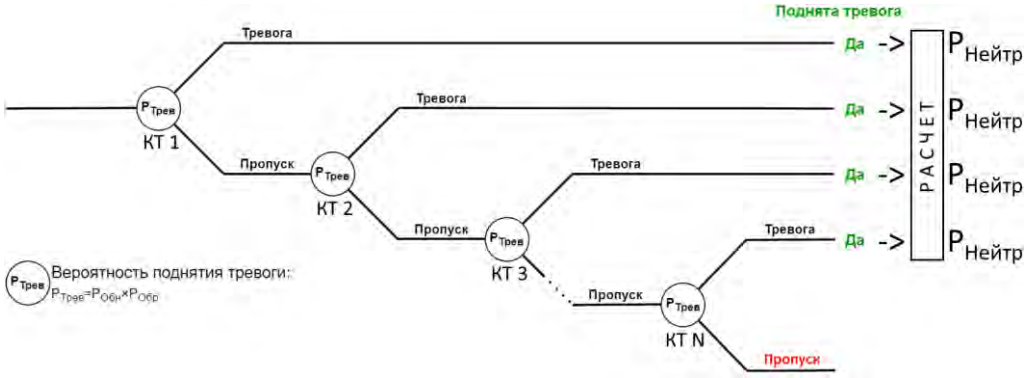

Рис. 2 – Сценарная последовательность воздействия нарушителя на КТ СФЗ

$$P_{Нейтр} = P_{Обн} \cdot P_{Обр} \cdot \int_0^{\infty} \frac{1}{\sqrt{2\pi\sigma_x^2}} \exp\left[-\frac{(x-\mu_x)^2}{2\sigma_x^2}\right] dx, \quad (1)$$

где μx – математического ожидание нормального распределения для интервала времени между сигналом тревоги и перехватом, а σ_x^2 – среднеквадратическое отклонение.

Таким образом, движение нарушителя через территорию охраняемого объекта – это некий путь через череду ключевых точек, обычно определяемых на препятствиях (охранных извещателях, ограждениях, развилках и т.д.). А реакция системы – это ответные действия по предотвращению продвижения нарушителя, описываемые формульным способом или сценарием движения охранников (путь по их ключевым точкам). Вместе эти две части (путь нарушителя и путь охранников) в общем представлении являются сценарием атаки на охраняемый объект. Такое представление сценария минимально необходимо для проведения вычислительного эксперимента. Но кроме этих двух составляющих в нѐм могут принимать участие множество других параллельных сценарных процессов: действия операторов службы безопасности, патрулирование объекта, воздействие погодных условий и т.д. – всѐ это оказывает влияние на общий сценарий, повышая как его реалистичность, а значит и точность для определенных условий.

Описанный выше сценарий представляет предопределенную последовательность КТ, а это значит – работу по формированию сценария со стороны эксперта по анализу уязвимости. При этом, для получения точных результатов требуются сложные сценарии (выше степень реалистичности), что влечѐт увеличение объѐма и сложности математических расчетов, а также требует рассмотрения различных вариантов сценариев для повышения объективности количественной оценки качества СФЗ для всего объекта в целом, а не только по одному варианту событий. Это увеличивает объем работы в геометрической прогрессии.

Для частичной автоматизации работы по созданию сценариев применяют подход с применением графов путей атак нарушителя. Такие графы могут описывать структуру СФЗ с помощью узловых точек (формировать цифровой двойник) или формировать покрытие доступного для передвижения пространства на территории цифрового двойника объекта (граф путей) [7]. В зависимости от выбранного графа будет определена подробность описания системы и еѐ абстракция.

Под абстракцией подразумевается, что цифровой двойник СФЗ может быть описан как обобщенными признаками подсистем и компонент в еѐ структуре (например, «периметр», «блок-пост» и т.д.) – критическими элементами [4], так и на уровне еѐ элементарных структурных компонентов и их параметров (извещателей, ограждений, охранников, видеокамер и т.д.). В первом случае – система описана как совокупность реакций по направлением атак нарушителя по графу, во втором случае – осуществляется имитация движения нарушителя по графу с взаимодействием с элементами, встреченными на пути (как на узловых точках, так и на ребрах графа).

Эксперт каким-либо образом задает граф путей для нарушителя. Каждый отдельный сценарий атак нарушителя на графе определяется либо вручную, либо с помощью какого-либо алгоритма: от алгоритмов поиска кратчайшего пути на графе [3] до генетических алгоритмов с использованием нечетких множеств [8]. Размерностью графа определяется сценарный масштаб системы и подробность путей атак нарушителя.

Проблемы существующих решений

Если для предопределенного сценария (подход № 1) удается получить наиболее быстрые результаты расчетов (производятся математические вычисления, например, расчет марковских цепей), то недостатком является то, что такой сценарий позволяет оценить качество СФЗ только в определенных условиях и по одному конкретному направлению атаки. Данный сценарий может быть полезен при исследовании уже известных уязвимостей в структуре СФЗ, по которым могут быть совершены атаки, но не для поиска таких слабых мест. При этом, для оценки всей структуры СФЗ в общем потребуется большое количество предопределенных сценариев по разным направлениям атак, и чем больше система – тем больше требуется сценариев.

Сценарии атак на основе графов (подход № 2) имеют большую гибкость, так как предполагают множество сценариев из комбинаций различных вариантов путей движения по узловым точкам. Комбинаторным путѐм можно перебрать все возможные варианты сценариев по графе, либо задать алгоритмы, которые произведут отбор направлений атак по графу (например, на ориентированном графе). Однако, как уже упоминалось в предыдущем разделе статьи, важен уровень абстракции. Часто высокий уровень абстракции позволяет получить быстрые результаты, которые могут лечь в основу рекомендаций к СФЗ, но при этом не будут являться еѐ реальными характеристиками из-за низкого уровня соответствия реально существующей системы со всей еѐ сложностью. Детальное описание цифрового двойника СФЗ с помощью увеличения сложности графа или подробности графа путей на объекте большой

площади влечет увеличение количества вводимых исходных данных сценариев в геометрической прогрессии.

Не смотря на преимущество сценариев на основе графов (подход № 2) перед предопределенными сценариями (подход № 1), их количество ограничено этим графом. Каждый вариант сценария по своей идее так же является предопределенным в рамках доступных нему узловых точек графа, а количество вариантов является ограниченным.

Кроме того, возникают сложности при попытках моделирования сценариев, описывающих действия охранников на территории объекта и их взаимодействие с нарушителем, пытающимся скрыться. Такой подход требует динамически изменяемых сценариев, не предсказуемых по своему ходу событий до момента окончания вычислительного эксперимента, что характерно для имитационного моделирования. Для этого цифровой двойник СФЗ должен быть представлен на основе математических моделей базовых элементов (а не набором узловых точек графа с параметрами). Над этим двойником проводится имитационный эксперимент с агентными моделями нарушителя и охранников, способными взаимодействовать друг с другом и элементами СФЗ на локальном уровне [9].

Таким образом, существует актуальная потребность в методах формирования сценариев, позволяющих:

− увеличить многообразие вариантов сценариев атак на охраняемый объект через цифровой двойник СФЗ,

− динамически изменять ход событий в эксперименте из-за возникновения каких-либо сценарных событий на основе вероятностных характеристик (проводить имитационное моделирование),

− автоматизировать работу эксперта над созданием сценариев и отнести его роль на этап оценки результатов.

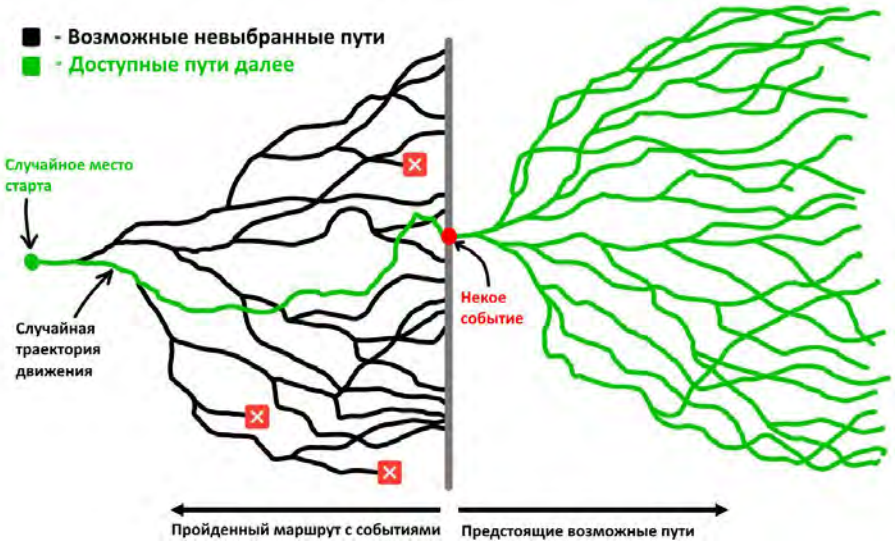

Рис. 3 – Иллюстрация динамического сценария в ходе статистического эксперимента с проникновением, иллюстрирующая непредсказуемый ход развития событий

Создание сценариев с помощью алгоритма событийно-управляемых траекторий

Необходимо выбрать подход, позволяющий не исследовать предопределенные последовательности событий при создании сценариев. Такой подход заранее ничего не будет знать о существовании заранее заданного пути или какого-либо графа, а будет руководствоваться синтезом свободно проложенной траектории (каким-либо алгоритмом поиска пути без графов, например, эвристическим [10]) и точек пересечения различных зон и элементов СФЗ этой траекторией. Таким образом, сценарий будет формироваться на основе некой траектории, проложенной по определенной логике (например, кратчайший маршрут), нарезанной на фрагменты точками пересечения зон элементов СФЗ в пространстве. Разделение траектории будет происходить по фактическим точкам пересечения в пространстве (2D или 3D) важных для моделирования элементов СФЗ, такие как зона обзора видеокамеры, зона видимости охранника, зона обнаружения датчика, полотно ограждения и т.д.

То есть, каждый фрагмент траектории будет соответствовать движению нарушителя в пространстве с определенным типом взаимодействия с СФЗ, а вероятностные события в результате этих взаимодействий будут разыгрываться в точках перехода фрагментов и в заданные моменты движения по ним. Пример можно увидеть на рисунке 4.

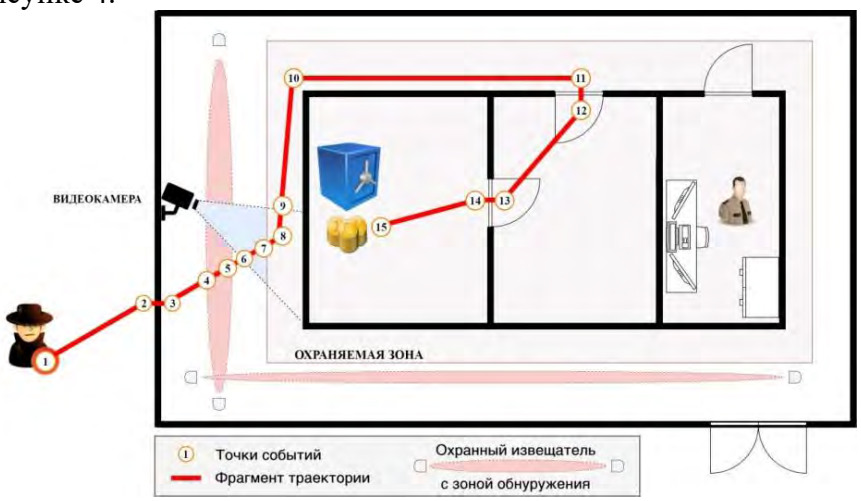

Рис. 4 – Траектория проникновения нарушителя, разбитая на множество фрагментов событиями (особые точки) от старта (точка 1) до финиша (точка 15)

Разбитый на фрагменты перемещения и точки переходов между ними путь, уже сам по себе, будет сценарием, который может быть описан как идентичный подходу предопределенных сценариев. Характер этого сценария будет зависеть от входных условий и той траектории, которая была сгенерирована прокладчиком для них. В практике применяются различные алгоритмы поиска пути без графов, которые сами по себе формируют граф во время генерации (например, простейший граф видимости на каждой итерации алгоритма поиска пути) [11, 12].

Динамические изменения сценария (его изменение) проникновения могут быть описаны с помощью вероятностных событий изменения поведения или пути проникновения к цели (нарушитель) / движения к нарушителю (охранник). Это значит, что по ходу выполнения сценария в какой-то момент произошло «некое событие» (см. рис. 3, например, нарушитель увидел охранника), вызывающее розыгрыш вероятности изменения сценария (нарушитель решает отбежать подальше или продолжить движение без изменений). В случае, если сценарий требуется изменить, то вызывается

прокладчик траекторий, который по заданным условиям (например, координата уклонения от охранника) строит новую траекторию, которая так же нарезается элементами цифрового двойника объекта на фрагменты перемещения со своими уникальными событиями.

Таким образом, алгоритм событийно-управляемых траекторий (АСУТ) представляет собой кооперацию работы прокладчика траекторий и алгоритма, формирующего фрагменты пути проникновения на этой траектории как на рисунке 3. Представить работу алгоритма можно с помощью блок-схемы (рисунок 5).

Рис. 5 – Блок-схема работы алгоритма событийно-управляемых траекторий

Каждый фрагмент траектории – это сценарное действие нарушителя (на пути проникновения до цели) или охранника (на пути перехвата нарушителя или к месту последней тревоги). На входах и выходах фрагментов осуществляется генерация сценарных событий (например, вход в зону обнаружения видеокамеры N), в результате которых может произойти розыгрыш вероятностных событий, постепенно задающих динамику развития сценария: вероятность обнаружения техническими устройствами, вероятность изменения траектории движения, вероятность принятия решения обойти преодолимое препятствие, подкопаться под ним, перелезть через него, прорезаться сквозь и т.д. Такой подход можно реализовать с помощью гибридных автоматов [9]. Пример сценария в виде UML-схемы можно увидеть на рисунке 6. Отличительные особенности и преимущества АСУТ в задачах генерации сценариев

Сценарий, получаемый с помощью АСУТ, представляет собой последовательность событий на пути движения нарушителя. Эти события оказывают влияние как на СФЗ (вызывая еѐ реакцию и ответные сценарии действий охранников), так и на поведение самого нарушителя: его скорость, осторожность и направление. Этого достаточно для проведения экспериментов с цифровым двойником СФЗ с целью сбора и анализа статистических данных результатов с целью формирования

количественных оценок качества. Оценки, получаемые в результате экспериментов по сценариям АСУТ, обладают большей прозрачностью (прослеживаются все последовательности действий нарушителя и охранников приближенно так, как это происходит в реальной жизни).

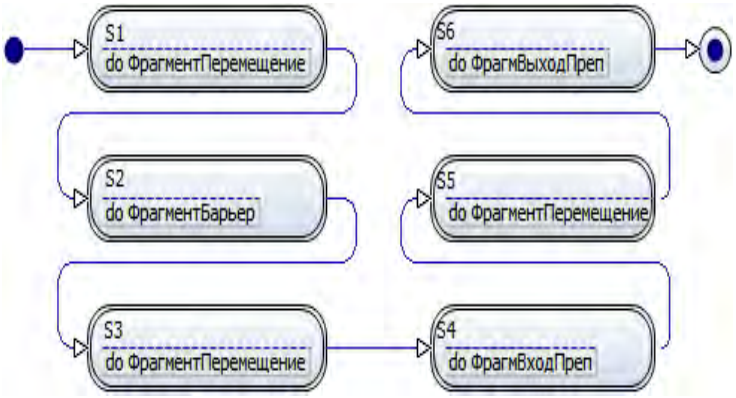

Рис. 6 – Фрагменты траектории в простом сценарии движения нарушителя через барьер и препятствие

Для своей реализации подход генерации сценариев проникновения с помощью АСУТ требует:

1) прокладчик траекторий, не использующий заранее заготовленные графы, способный выдавать траекторию по координатам через цифровой двойник СФЗ; это может быть эвристический алгоритм, например, Polaris;

2) использование гибридных автоматов для формирования сценарных последовательностей, событиями в которых являются взаимодействие человека и СФЗ, а также логико-вероятностные характеристики, описывающие поведение этого человека.

Реализация алгоритма событийно-управляемых траекторий удовлетворяет актуальным требованиям, выдвигаемым к сценариям для проведения имитационных экспериментов:

1) увеличивается многообразие вариантов неповторяющихся сценариев атак нарушителя и реакций СФЗ, которые не удастся составить на основе проникновения по графам;

2) сценарии являются динамически изменяемыми при наличии вероятностных событий, влияющих на последующие действия нарушителя; причем все последующие события будут полностью независимы от уже свершившихся (не предопределѐнный эксперимент, который нельзя рассчитать с помощью марковских цепей);

3) отпадает необходимость в использовании заранее заданного графа для проведения имитационного эксперимента; это автоматизирует работу специалистов по созданию сценариев, сводя еѐ только к заданию стартовых, внешних и конечных условий проведения имитационного эксперимента (место возникновение нарушителя, модель нарушителя, погодные условия, цель проникновения и т.д.);

4) вычислительная сложность генерации сценариев с помощью АСУТ значительно ниже, чем для крупномасштабных моделей на основе графов; при этом, результаты экспериментов по таким сценариям обладают не меньшей подробностью, а порой превосходят аналогичные по сценариям на графах.

Выводы

Предлагаемый подход является совершенствованием существующих способов создания сценариев проникновения для проведения вычислительных экспериментов с целью получения количественных оценок качества СФЗ. АСУТ учитывает и преодолевает перечисленные выше недостатки сценариев, получаемых на основе графов.

Результаты практической разработки АСУТ применены в программном комплексе «АКИМ» (ООО ПЕНТАКОН) [13,14], разработанном для создания математических моделей СФЗ и проведения над ними имитационных экспериментов с проникновением нарушителя с целью сбора статистических данных исходов и формирования количественной оценки качества СФЗ.

Литература

1. **Леус А.В.** Оценка эффективности систем безопасности с помощью моделирования перемещения субъектов движения по охраняемому объекту: дис. канд. технич. наук: 05.13.01. М., 2012. 129 с.
2. **Степанов Б.П., Годовых А.В.** Основы проектирования систем физической защиты ядерных объектов: учебное пособие // Томский политехнический университет. Томск: Изд-во Томского политехнического университета, 2009. С. 67-118.
3. **Шанаев Г.Ф., Леус А.В.** Системы защиты периметра. М.: Секьюрити Фокус, 2011. 280 с.
4. **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.
5. **Мосолов А.С.** Оценка эффективности системы безопасности на основе метода Монте-Карло // Журнал "Системы безопасности". 2014. № 1
6. **Sasser D.W.** Users guide for EASI graphics - Sandia Labs., 1978 Albuquerque, N.Mex. (USA). С. 37-39.
7. Программное обеспечение «ИТЕРАЦИЯ – МОДЕЛЬ СФЗ 2.0» Руководство оператора // Итерация URL: https://iter.ru/model_sfz.html (дата обращения: 15.09.2022).
8. **Боровский А.С.** Модели, методы и алгоритмы интеллектуальной поддержки принятия решений в задачах разработки и оценки систем физической защиты объектов информатизации: дис… докт. техн. наук: 05.13.19. Оренбургский государственный аграрный университет, Оренбург, 2015. 344 с.
9. **Шарков И.К., Сениченков Ю.Б., Колесов Ю.Б.** Моделирование и оценка качества систем физической защиты на основе агентного подхода и алгоритма событийно-управляемых траекторий // Сборник трудов конференции «ИММОД – 2021». СПб.: 2021. С. 503-510.
10. **Шарков И.К., Желудков Е.А.** Применимость эвристического алгоритма для задач поиска траекторий движения через систему физической защиты // SEIM-2019. СПб.: 2019. С. 34-40.
11. **Фурсов В.В., Самохвалова С.Г.** Анализ алгоритмов поиска пути для различных задач и их использование в мобильном приложении // Вестник Амурского государственного университета. Серия: Естественные и экономические науки. 2017. №77.

12. **Федоров А.А., Сошилов И.В., Логинов В.Н.** Эвристические алгоритмы поиска маршрутов передачи данных в спутниковых системах и их валидация // Труды МФТИ. 2020. №3 (47).
13. **Шарков И.К., Крылов В.М.** Планирование и оценка качества систем физической защиты с помощью имитационного моделирования // Сборник трудов конференции «ИММОД – 2021». СПб.: 2021. С. 496-502.
14. **Шарков И.К.** Имитационное моделирование средств физической защиты на охраняемом объекте в задачах оценки уязвимости // Сборник трудов конференции «ИМСВН – 2020». СПб.: 2020. С. 254-264.