УДК 519.876.5 doi: 10.15827/0236-235X.149.077-088 2025. Т. 38. № 1. С. 77–88

Имитационное моделирование систем физической защиты в среде АКИМ

Ю.Б. Сениченков [1], **И.К. Шарков** [2] ✉

[1] Санкт-Петербургский политехнический университет Петра Великого, г. Санкт-Петербург, 195251, Россия
[2] Компания ПЕНТАКОН, г. Санкт-Петербург, 197198, Россия

Ссылка для цитирования
Сениченков Ю.Б., Шарков И.К. Имитационное моделирование систем физической защиты в среде АКИМ // Программные продукты и системы. 2025. Т. 38. № 1. С. 77–88. doi: 10.15827/0236-235X.149.077-088
Информация о статье
Группа специальностей ВАК: 2.3.1
Поступила в редакцию: 02.05.2024 После доработки: 23.07.2024 Принята к публикации: 13.08.2024

Аннотация. В статье обсуждается методика построения имитационных моделей в отечественном программном комплексе АКИМ. Модели предназначены для решения задачи анализа защищенности существующих и проектируемых систем физической защиты объектов и для формирования оценок их эффективности с помощью статистического эксперимента. Приводится обзор существующих современных подходов к решению аналогичной задачи. Большинство из них применяют марковские цепи для поиска уязвимых путей и графы атак и защит для оценки эффективности системы. В качестве альтернативы предлагается строить имитационную модель без построения графа атак и защит, опираясь только на план системы физической защиты. Модель в среде АКИМ создается из экземпляров базовых классов, моделирующих реальные элементы системы физической защиты, в результате чего возникает план, по которому будут двигаться модели агентов и охранников, имитируя реальные атаки. Подход позволяет подробно описывать функции, реакции и возможности системы на уровне ее элементов и задавать фактические параметры нарушителей и охранников, что обеспечивает точность и полноту анализа без упрощений или исключения важных деталей. На демонстрационных примерах показано, что оценки эффективности моделей защиты систем, полученные с помощью программного комплекса АКИМ, близки к оценкам эффективности моделей систем, построенных с помощью марковских цепей. При этом рассматриваемый метод построения имитационных моделей позволяет преодолевать трудности, связанные с использованием марковских цепей: необходимость использовать экспертные оценки коэффициентов матрицы переходов, матрицы большого размера, сложности модификации модели.

Ключевые слова: имитационное моделирование, система физической защиты, агентное моделирование, цепи Маркова, оценка эффективности, атака нарушителя, алгоритмы поиска пути

Благодарности. Автор выражает глубокую благодарность и признательность своему научному руководителю доктору технических наук Юрию Борисовичу Сениченкову, соавтору, безвременно ушедшему в октябре 2024 года

Введение. Обеспечение физической безопасности на территориях объектов повышенной важности, таких как аэропорты и топливно-энергетические комплексы, является важной задачей. Для ее выполнения применяются *системы физической защиты* (СФЗ), включающие инженерно-технические и человеческие ресурсы для защиты от различных угроз. Эффективность СФЗ определяется такими критериями, как вероятность обнаружения и нейтрализация нарушителей.

Современным способом оценки эффективности систем является компьютерное моделирование. Различные методики построения компьютерных моделей СФЗ и проведения статистических экспериментов с ними позволяют количественно оценить защищенность объектов, описать сильные и слабые стороны системы с помощью различных измеряемых характеристик, что способствует принятию обоснованных решений при проектировании или модификации СФЗ.

Задачи создания моделей, учитывающих все значимые особенности защищаемых объектов, и построения реалистичных сценариев атак и защит являются ключевыми в области оценки эффективности существующих или проектируемых СФЗ.

Методы построения моделей СФЗ

В основе многих современных методик оценки эффективности систем защиты периметра заложены требования МАГАТЭ, учтенные в методике EASI (США, 1977). Методика EASI предлагает рассматривать только один заданный сценарий внешнего воздействия на систему, в котором последовательность событий (атака, обнаружение, локализация нарушителя и его захват) сопровождается последовательностью вычислений, базирующихся на вероятностях обнаружения нарушителя, на правильной реакции и своевременном прибытии охраны.

Главные недостатки этого подхода – наличие только одного сценария атаки и заданные экспертом значения исходных параметров модели (вероятностей событий). Они не дают возможность достоверно оценить эффективность защиты всего объекта.

Подходы к преодолению указанных недостатков можно разбить на несколько групп по способу формирования моделей из плана охраняемого объекта. Эти модели позволяют создавать множество различных сценариев атак и защит и уменьшать влияние субъективного мнения эксперта на основе

– формирования графа атак и защит вручную экспертом;

– параметрического чертежа (карты) системы и соответствующего ему графа атак;

– параметрического чертежа, на котором разыгрываются различные варианты атак агентов и защиты, без использования явно заданного графа атак и защит.

Перечисленные подходы к формированию моделей используются в программных комплексах различного назначения, преимущественно для оценки существующих систем и реже для их проектирования.

Модели на основе заданного экспертом графа. Представление модели системы защиты на основе графа атак является классическим решением. За основу берется предложенный экспертом граф атак [1], построенный для упрощенной системы, и строятся все возможные пути атак. Для оценки эффективности системы чаще всего применяется методика EASI для каждого пути и автоматически строится оценка для всей системы.

Для повышения достоверности оценки необходимо также применять методики и алгоритмы анализа СФЗ, которые способны имитировать действия агентов-нарушителей, охранников и операторов при взаимодействии с системой и друг с другом.

Существуют примеры имитации взаимодействия связи между охранниками и операторами безопасности, в которых применяется метод [2] на основе модифицированной методики EASI. Этот метод, в свою очередь, не учитывает человеческий фактор, связанный с взаимодействием атакующих нарушителей и охранников. Попытка учесть человеческий фактор описана в работах [3, 4], авторы которых использовали генетические алгоритмы для имитации действий нарушителя и нечеткие множества описания допустимых параметров.

В работах [5, 6] предлагается формировать возможные пути атак с учетом базового типа нарушителя, созданного в соответствии с категорией объекта (ГОСТ Р 78.36.032-2013).

Первый (и главный) недостаток оценки эффективности системы по созданному вручную графу заключается в том, что приходится упрощать структуру моделируемой системы. Это приводит к появлению упрощенных сценариев атак, а упрощения непосредственно влияют на достоверность результатов оценки.

Второй недостаток – не всегда понятно, как на основе модели, предложенной экспертом, построить план реальной системы (чертеж), если речь идет о проектировании новых систем. В работае [7] предлагается строить план по уже существующему графу атак и оснащения модели инженерно-техническими средствами. Однако при данном подходе главный недостаток – синтез реальной сложной системы на основе упрощенной модели графа атак, не учитывающей все возможные реальные пути атак и зависящей от субъективного мнения эксперта, – остается. С организационной точки зрения требуются подготовленный специалист для построения модели (графа) и проектировщик, рисующий чертеж и проверяющий систему на соответствие нормативным требованиям, что разделяет всю работу по анализу, оценке эффективности и синтезу планируемой системы на два сложных этапа.

Третий недостаток – сложность описания крупномасштабных систем, где количество вероятностных переходов и состояний будет огромным, а следовательно, при создании такой модели потребуются значительные усилия.

Модели на основе параметрического плана и графа атак. В качестве первоначальной информации об объекте предлагается использовать его параметрический план. По этому плану создается граф атак: автоматически с использованием специальной объектно-ориентированной модели системы (*Building Information Model*, BIM) и специальных алгоритмов [8] или при помощи промежуточной модели атак в виде сетки перемещения [9, 10], наложенной на план объекта.

В обоих случаях при каждом значимом изменении структуры системы приходится заново строить граф, что повышает трудоемкость проектирования.

Недостатком моделей на основе BIM является зависимость от стороннего ПО, поэтому на практике чаще применяются подходы с наложением сетки. Они реализованы в отечественных программных продуктах ВЕГА-2, ИТЕРАЦИЯ-СФЗ и зарубежном IPAD.

Применение модели на основе сетки перемещения требует использования специальных эвристических алгоритмов поиска пути, что затрудняет моделирование систем с большой площадью и сложностью. В таком случае опять же приходится упрощать структуру графа (например, увеличивать размер ячеек сетки) и искажать траектории движения нарушителя и охранника, что приводит к очередному упрощению сценариев атак и влияет на достоверность оценки эффективности системы защиты.

Модели на основе карты (параметрического чертежа) и имитации атак и защиты агентов. Публикаций, посвященных этому методу и его реализациям в современном ПО, довольно мало.

План реализуется в виде двухмерной или трехмерной карты с пространством для имитации перемещения агентов атаки и защиты. Система физической защиты является иерархической моделью, каждый компонент которой представлен в виде ее базовых элементов (датчиков, камер, ограждений и т.д.) со своими уникальными параметрами, а агенты своими уникальными моделями.

Вместо построения графа атак и анализа всех его путей разрабатываются и применяются алгоритмы, имитирующие движение нарушителей и охранников по карте системы. Эффективность системы защиты определяется с помощью статистических экспериментов.

В работе [11] имитационная модель строится на основе игровой модели с применением стороннего ПО (ARMA3), в котором осуществляется имитация атак на объекты ядерной энергетики. В [12] обсуждаются возможности построения имитационных моделей на основе теории игр.

Предлагаемый подход. Способ построения цифрового двойника системы защиты и графический язык моделирования, позволяющий создавать чертеж проектируемой системы и проводить статистические эксперименты, имитируя проникновение агентов-нарушителей и противодействие агентов-защитников, описаны в [13, 14].

Данный подход отличается от описанных выше прежде всего тем, что не использует заранее заданный или автоматически построенный граф атак, а требует только чертеж исследуемой системы, включающий существующие, библиотечные, компоненты: модели устройств, созданных на основе их паспортных данных, модели охранников и операторов с алгоритмами имитации их движения.

В отличие от подхода, предлагаемого в [7], процесс построения модели системы начинается с проектирования чертежа и не требует участия специально обученного специалиста в области моделирования. Предлагаемый подход помогает найти уязвимые места системы и улучшить ее свойства. Для этого достаточно изменить чертеж (исходную модель) и повторить статистический эксперимент.

Подход на основе марковских цепей используется многими авторами [15–17], поэтому сравним его с методом, применяемым в среде АКИМ.

Построение имитационной модели СФЗ на базе графов атак

Граф атак можно использовать как основу имитационной модели, в которой каждая возможная атака (сценарий атаки) реализуется с помощью случайного выбора ребра при движении от текущего узла до следующей локальной цели. Новые сценарии формируются и реализуются до тех пор, пока оценки вероятности задержания агента и уничтожения объекта не будут вычислены с необходимой точностью. Такой подход позволяет избежать решения уравнений, однако сами матрицы переходов приходится строить и хранить даже при использовании имитационной модели.

Приведем пример использования имитационной модели на базе графа атак, реализованной в среде AnyDynamics (https://www.mvstudium.com/advan.htm).

Моделируемая СФЗ объекта, окруженного стеной с одним КПП, представляется графом атак (http://www.swsys.ru/uploaded/image/2025-1/5.jpg), который реализуется в виде карты поведения (упрощенной машины состояний UML), формирующей очередной сценарий, с помощью матрицы переходов (рис. 1).

Строки матрицы соответствуют следующим состояниям: S1 – начальное состояние, где случайным образом осуществляется выбор атаки через КПП (S2) или нескольких вариантов преодоления стены (S3, S4, S5); S6, S7 – вспомогательные состояния, позволяющие сократить число путей в S8 (захват охраной агента) и S9 (достижение агентом цели (проигрыш защиты)).

Имитационная модель на языке карт поведения представлена циклом (http://www.swsys.ru/uploaded/image/2025-1/6.jpg), многократно повторяющим (Nexp) отдельный эксперимент.

$$A=\begin{bmatrix}0 & \frac{1}{20} & \frac{3}{20} & \frac{1}{5} & \frac{3}{5} & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & \frac{1}{10} & \frac{9}{10}\\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & \frac{3}{10} & \frac{7}{10}\\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0\\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1\end{bmatrix}\begin{array}{l}-\mathbf{S1}\\ -\mathbf{S2}\\ -\mathbf{S3}\\ -\mathbf{S4}\\ -\mathbf{S5}\\ -\mathbf{S6}\\ -\mathbf{S7}\\ -\mathbf{S8}\\ -\mathbf{S9}\end{array}$$

Рис. 1. Матрица переходов (параметр A в модели AnyDynamics), где состояния S2–S5 имеют безусловные переходы к другим, а S8, S9 конечные

Fig. 1. Transition matrix (parameter A in AnyDynamics model), where states S2-S5 have unconditional transitions to others and S8, S9 are finite

Можно непосредственно решить уравнения, одновременно реализовать имитационную модель и увидеть, что результаты вычислений, как и следовало ожидать, совпадают до третьего знака.

Имитация движения нарушителя по плану СФЗ без заданного графа

Имитационную модель можно создать, не строя граф атак и защит, опираясь только на план СФЗ. Такой подход реализован в комплексе экспертного моделирования АКИМ. Подход позволяет подробно описывать функции, реакции и возможности системы на уровне ее элементов и задавать фактические параметры нарушителей и охранников, что обеспечивает точность и полноту анализа без упрощений или исключения важных нюансов. Это особенно полезно для проектирования систем, так как созданный цифровой двойник объекта служит одновременно графическим образом и параметрическим планом в виде чертежа для проектной документации.

Модель в АКИМ строится из экземпляров базовых классов, моделирующих реальные элементы СФЗ, в результате чего возникает план, по которому будут двигаться модели агентов и охранников, имитируя реальные атаки (http://www.swsys.ru/uploaded/image/2025-1/7.jpg). Классы могут использовать базовые элементы средств защиты, например, извещатели (датчик), видеокамеры, ограждения и т.д. Модели средств защиты содержат параметры, соответствующие техническим паспортам устройств, и их геометрическую форму зон воздействия с привязкой к плану СФЗ.

Имитация атак осуществляется с помощью алгоритма, прокладывающего локальные отрезки пути по плану от текущей точки до следующей достижимой, и алгоритма, учитывающего влияние событий на форму выбранного локального пути.

Для прокладки локального отрезка пути используется эвристический алгоритм поиска пути между двумя точками на плане с учетом видимых препятствий. Для выбора варианта обхода отдельного непреодолимого препятствия на пути атаки используется локальный граф видимости. Под ним подразумевается граф путей обхода одного препятствия с учетом его видимых вершин. Такой граф автоматически строится для каждого встреченного препятствия, и с его помощью строится кратчайший маршрут обхода.

Алгоритм формирования событийно-управляемых траекторий расставляет случайные события на локальном отрезке пути, и возникает событийно-управляемая траектория, формируемая с помощью гибридных автоматов. Это позволяет автоматически строить динамические сценарии экспериментов и исключать необходимость привлечения эксперта на этапе подготовки модели СФЗ. Случайные события влияют на выбор агентом очередной достижимой точки (смена локального отрезка пути под воздействием событий), что вносит случайные изменения в сценарий.

Взаимодействие прокладчика пути и алгоритма формирования событийно-управляемых траекторий можно представить в виде схемы (рис. 2).

Сценарии разыгрываются многократно, что позволяет собирать подробную статистику обо всех событиях и моделируемых значениях в ходе каждого испытания. С помощью доверительных интервалов определяется критерий для ограничения количества испытаний в серии, что обеспечивает достоверную оценку эффективности СФЗ:

– вероятность обнаружения с помощью ТСО ($P_{\text{Обн}}$);

– вероятность нейтрализации нарушителя ($P_{\text{Нейтр}}$);

– наиболее уязвимые траектории (пути и координаты);

– время задержки нарушителя на ИСО (t) и другие.

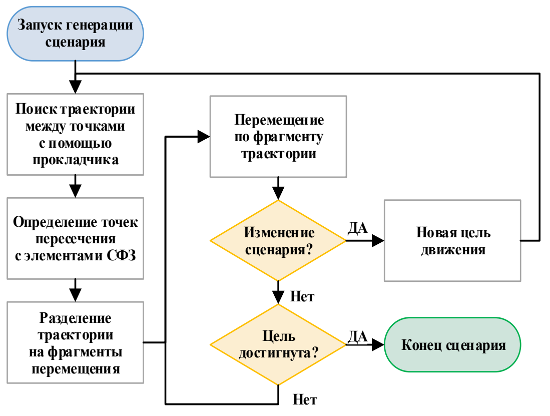

Рис. 2. Схема взаимодействия прокладчика пути и алгоритма для формирования динамически изменяемого сценария эксперимента

Fig. 2. Schematic interaction between the path planner and the algorithm for a dynamically changing experiment scenario

Сравнение подходов: одномерная модель системы

Сравним различные модели СФЗ на основе марковских цепей и моделей, реализованных в среде АКИМ. Рассмотрим одномерную модель СФЗ (последовательные события), показывающую путь нарушителя через зону досмотра в аэропорту при посадке на самолет.

Обычно одномерные модели не принято моделировать с использованием марковских цепей. Для них существует международная методика МАГАТЭ EASI. Эта методика оценивает на одном заданном пути атаки вероятность обнаружения и своевременного прибытия охранников (нейтрализации) к месту тревоги.

Одномерную модель можно реализовать в виде простой карты поведения (http://www.swsys.ru/uploaded/image/2025-1/8.jpg).

Результаты моделирования показали, что вероятность успешной защиты СФЗ составила 0.844, а вероятность провала – 0.155 (http://www.swsys.ru/uploaded/image/2025-1/9.jpg).

Помимо оценки вероятностей успешной защиты и ее провала, среда АКИМ позволяет

– рисовать чертеж СФЗ, учитывающий реальную геометрию объекта (расположение всех его базовых элементов средств охраны в пространстве на пути атаки);

– прокладывать траекторию движения агента по созданному чертежу, представляющему собой цифровой двойник реального пространства СФЗ со всеми ее характеристиками;

– автоматически формировать характеристики для заданной траектории атаки (длину пути, список препятствий/датчиков/видеокамер на пути с учетом сложности их преодоления);

– осуществлять движение агента по сформированной траектории с учетом реальных характеристик пути, имитируя реальное движение агента; реальные характеристики движения агента (скорость, время преодоления препятствия и т.д.) формируются на основе выбираемых проектировщиком законов распределения (http://www.swsys.ru/uploaded/image/2025-1/10.jpg), причем случайные характеристики, связанные с людьми, могут определяться PERT-распределением (четырехпараметрическим бета-распределением).

Рассматриваемая одномерная модель в АКИМ представлена на рисунке 3.

Модель атаки в среде АКИМ позволяет провести эксперимент, имитирующий реальное движение агента: агент движется со случайной скоростью на всех фрагментах пути атаки, затрачивая время не только на движение, но и на преодоление препятствий и взаимодействуя с зонами обнаружения технических средств охраны.

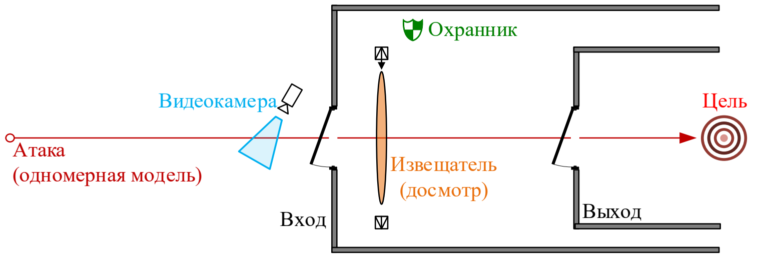

Рис. 3. Графическое отображение атаки нарушителя с заданной последовательностью событий на ее пути, как оно может представляться в среде АКИМ

Fig. 3. Graphical representation of an intruder attack with a given sequence of events on its path, as it can be represented in the AKIM environment

Аналогично моделируется реакция охранника, который, как и в реальной жизни, должен вовремя отреагировать на нарушение и приблизиться к атакующему агенту. Успешная защита объекта возможна только в случае, если время движения охранника к нарушителю ($T_{Охр}$) меньше времени движения агента ($T_{Нар}$) до цели [11].

Параметры модели в среде АКИМ:

– скорость нарушителя (от 1 до 12 км/ч);

– путь нарушителя от точки старта до цели (244 м);

– вероятность обнаружения нарушения через видеокамеру (P = 0.4);

– вероятность обнаружения нарушения через извещатель (P = 0.95);

– время на преодоление входных и выходных ворот (от 30 до 300 сек.);

– вероятность правильной реакции охранника (P = 0.9);

– время принятия решения охранником (от 1 до 30 сек.);

– координаты охранника относительно пути атаки;

– скорость движения охранника по направлению к нарушителю (от 8 до 20 км/ч).

Результаты моделирования в среде АКИМ для 1 000 испытаний дали 957 успешных нейтрализаций нарушителя, что попадает в доверительный интервал от 0.9444 до 0.9696. Точечная вероятность составила 95.7 %, а обнаруживающая способность системы технических средств охраны – около 98.5 %.

Оценки вероятностей исходов для марковской цепи и имитационной модели среды АКИМ различаются на 11.3 %.

Сравнение подходов: двухмерная модель системы

Рассмотрим двухмерную модель СФЗ охраняемого объекта с двумя рубежами охраны и тремя охраняемыми КПП и сравним результаты моделирования с помощью марковской цепи и имитационной модели АКИМ.

Граф атак для марковской модели с использованием карты состояний (http://www.swsys.ru/uploaded/image/2025-1/11.jpg) даже для такой простой системы оказывается трудновоспринимаемым. Матрица переходов (рис. 4) разреженная, размерности 10.

Как имитационная модель для марковской цепи в виде графа атак, так и решение уравнений дают следующие оценки: вероятность успешной защиты системы (нарушитель пойман)

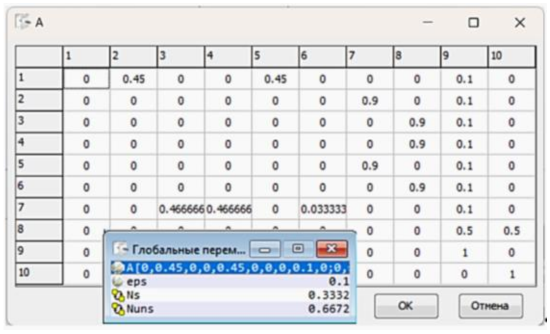

Рис. 4. Матрица переходов и результаты: Ns – провал защиты (нарушитель дошел до цели), Nuns – успешная защита (атакующий агент пойман), в конце – поглощающие состояния, соответствующие удачной и неудачной атакам

Fig. 4. Transition matrix and results: Ns – defense failure (the intruder reached the target), Nuns – successful defense (the attacker is caught), at the end – absorbing states corresponding to successful and unsuccessful attacks

составила 0.667, вероятность провала защиты (нарушитель достиг цели) – 0.333.

Имитационная модель среды АКИМ для этого плана представлена на рисунке 5, где показан процесс построения СФЗ с помощью базовых компонентов.

Для проведения экспериментов в среде АКИМ необходимо указать место появления атакующих агентов (http://www.swsys.ru/uploaded/image/2025-1/12.jpg). Это можно сделать различными способами, например: линию вокруг объекта (окружность, многоугольник или отрезок) разбить на участки, где может появиться агент, и случайным образом выбрать точку появления.

Первое отличие от марковской модели: вместо ограниченного количества сценариев, порождаемых графом путей для марковской модели, имитационная модель АКИМ строит уникальные пути атак и защиты, порождаемые случайным образом ранее описанными алгоритмами (рис. 2).

Результат построения таких уникальных путей атак из одной точки появления агента в разных экспериментах проиллюстрирован на рисунке 6.

Результаты моделирования по участкам возникновения нарушителя представлены в таблице 1.

Оценки вероятностей исходов для марковских моделей и имитационной модели АКИМ отличаются на 11.4 %. При этом на участке 11

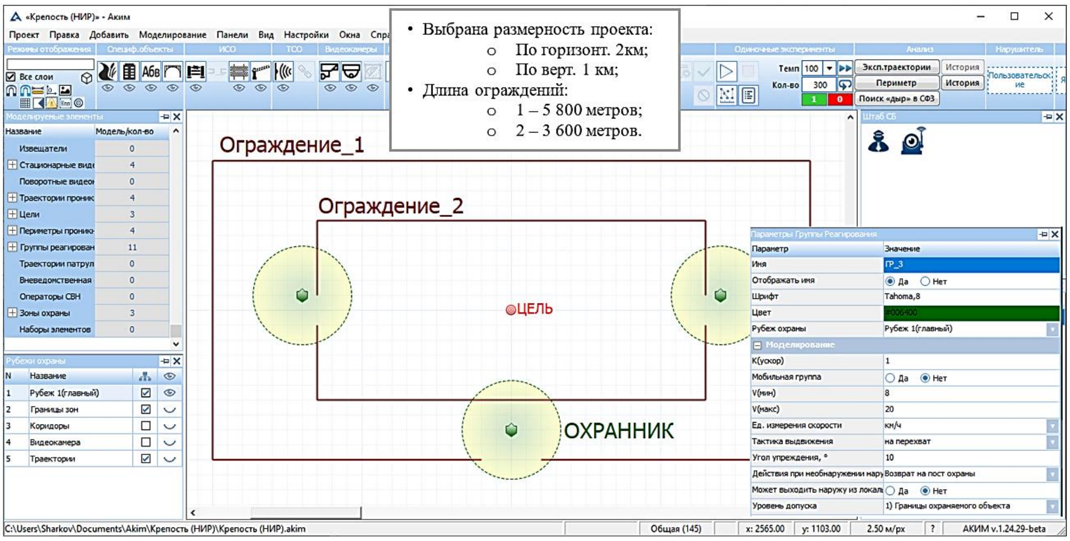

Рис. 5. Структура СФЗ в виде чертежа из базовых элементов, представленных отдельными моделями (ограждения, охранники, цель)

Fig. 5. Physical protection systems structure as a drawing of basic elements represented by separate models (fences, guards, target)

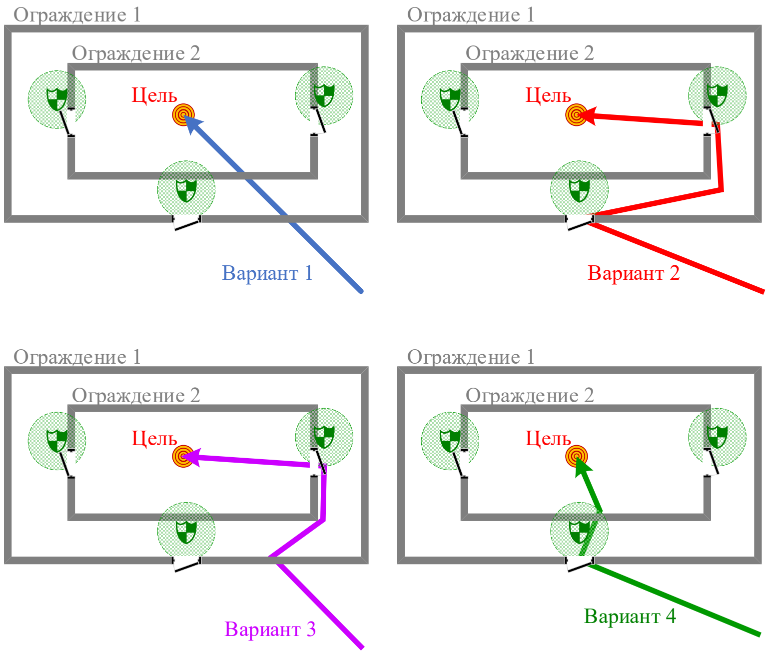

Рис. 6. Примеры построения случайных траекторий атак

Fig. 6. Examples of building random attack paths

оценка эффективности совпадает с марковской моделью (рис. 4).

Второе отличие от марковской модели: среда АКИМ предлагает описывать агента-нарушителя набором реальных количественных характеристик, влияющих на имитацию движения и, следовательно, на результаты моделирования. Такие характеристики может выбирать разработчик (рис. 7), создавая те или иные модели нарушителей, что недоступно для других методик.

Можно сравнить результаты моделирования с нарушителем «Дилетант» (не применяет специальные приспособления, облегчающие

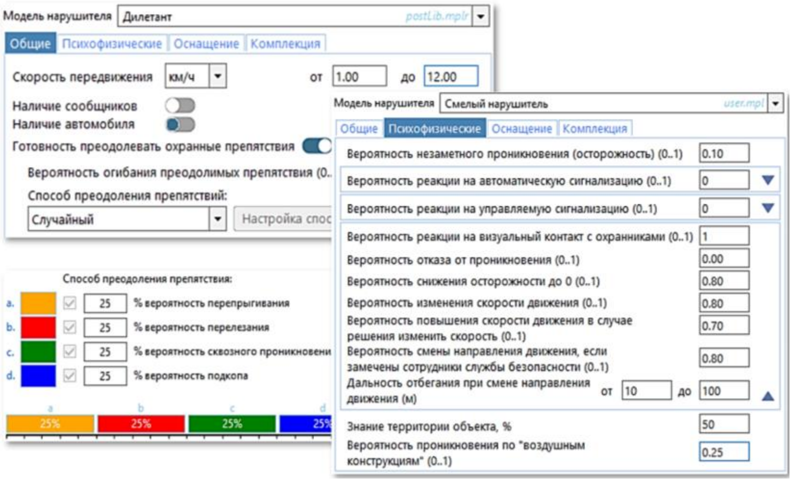

Рис. 7. Пример диалогов выбора характеристик для нарушителя

Fig. 7. Example of dialogs for selecting intruder's characteristics

ему проникновение, и готов отказаться от проникновения при виде охранника) (табл. 1) с результатами моделирования с «Нарушителем, применяющим силовой метод проникновения» (использует подручные средства и экипировку при атаке, не отказывается от проникновения в случае тревоги на объекте и обнаружения охранника) (табл. 2). Оценка вероятности нейтрализации для агента «Дилетант» (0.781) уменьшилась в полтора раза по сравнению с «Нарушителем, применяющим силовой метод проникновения» (0.473).

Для изменения модели поведения агента в марковской модели эксперту необходимо переопределять значения вероятностей в матрице переходов, опираясь на свой личный опыт, или прибегать к описанным в обзорном разделе методикам.

Третье отличие от марковской модели: среда АКИМ легко справляется с проблемой масштабирования размеров СФЗ (http://www.swsys.ru/uploaded/image/2025-1/13.jpg) и изменения ее структуры.

Чтобы оценить отличающийся по масштабам или пропорциям объект с помощью марковской цепи, потребуется переопределение значений вероятностей в матрице переходов. В среде АКИМ меняются только размеры эле-

Таблица 1

Результаты моделирования с моделью нарушителя «Дилетант»

Table 1

Simulation results with the "Amateur" intruder model

Участок	Количество испытаний	Количество успешных испытаний	Доверительный интервал
1	345	252	0.6836–0.7773
2	345	253	0.6867–0.7800
3	344	276	0.7602–0.8444
4	344	269	0.7383–0.8256
5	345	267	0.7298–0.8181
6	344	312	0.8763–0.9377
7	344	294	0.8174–0.8919
8	344	251	0.6827–0.7766
9	345	277	0.7609–0.8449
10	344	287	0.7950–0.8736
11	345	243	0.6562–0.7525
12	346	249	0.6723–0.7670

Примечание: минимальная вероятность поимки нарушителя составила 70.4 % (участок 1), общая вероятность поимки для всей СФЗ – 78.1 %.

ментов на карте, а все экспертные характеристики и данные из документации устройств остаются неизменными.

В таблицах 1 («Дилетант») и 2 («Нарушитель, применяющий силовой метод проникновения») приведены результаты оценки эффективности для территории СФЗ площадью 1.99 км^2, в таблице 3 – для территории площадью около 0.2 км^2 (агент «Дилетант»).

Вероятность нейтрализации нарушителя для СФЗ площадью 0.2 км^2 значительно выше, чем в предыдущих случаях, как и следовало ожидать.

Необходимо отметить, что реальная система будет во много раз сложнее, чем в пред-

Таблица 2

Результаты моделирования с моделью «Нарушитель, применяющий силовой метод проникновения»

Table 2

Simulation results with the model "Intruder using forced penetration"

Участок	Количество испытаний	Количество успешных испытаний	Доверительный интервал
1	1 000	485	0.4540–0.5160
2	1 000	454	0.4231–0.4849
3	1 000	528	0.4971–0.5589
4	1 000	495	0.4640–0.5260
5	1 000	456	0.4251–0.4869
6	1 000	433	0.4023–0.4637
7	1 000	420	0.3894–0.4506
8	1 000	451	0.4202–0.4818
9	1 000	478	0.4470–0.5090
10	1 000	542	0.5111–0.5729
11	1 000	463	0.4321–0.4939
12	1 000	466	0.4351–0.4969

Примечание: минимальная вероятность обезвреживания – 42.0 % (участок 7), общая вероятность обезвреживания – 47.3 %.

Таблица 3

Результаты для моделирования с моделью нарушителя «Дилетант» на объекте площадью 0.2 кв. км

Table 3

Results for simulations with the "Amateur" intruder model at a 0.2 square kilometer site

Участок	Количество испытаний	Количество успешных испытаний	Доверительный интервал
1	1 000	760	0.7335–0.7865
2	1 000	934	0.9186–0.9494
3	1 000	986	0.9787–0.9933
4	1 000	976	0.9665–0.9855
5	1 000	995	0.9906–0.9994
6	1 000	993	0.9878–0.9982
7	1 000	992	0.9865–0.9975
8	1 000	991	0.9851–0.9969
9	1 000	994	0.9892–0.9988
10	1 000	989	0.9825–0.9955
11	1 000	949	0.9354–0.9626
12	1 000	791	0.7658–0.8162

Примечание: минимальная вероятность обезвреживания составила 76.0 % (участок 1), общая вероятность обезвреживания – 94.6 %.

ставленном примере. Даже простейшая система может включать в себя десятки устройств обнаружения с разными характеристиками, множество охранников, сложную топографию пространства перемещения. Для моделирования такой системы с помощью марковских цепей неизбежно приходится упрощать модель, в противном случае усложнение модели приводит к экспоненциальному росту состояний и путей в графе только для одного атакующего агента (без рассмотрения множественных атак).

Заключение

Предложенный в статье агентный подход имитационного моделирования атак и защиты представляет собой более гибкое и более правдоподобное решение задачи оценки эффективности СФЗ, позволяющее учитывать широкий спектр возможных сценариев атак и характеристик нарушителей. В отличие от подхода с использованием марковских цепей данная имитационная модель не требует явного построения графа атак. Она дает возможность осуществлять детальную проработку модели, снижает субъективное влияние эксперта на входные данные, повышает объективность оценки и строит более реалистичные сценарии атак.

Таким образом, подход с имитацией движения агентов в цифровом двойнике системы, реализованном в виде реальных рабочих чертежей, является новым перспективным направлением в области планирования и оценки систем физической защиты.

Предлагаемая технология может применяться для проектирования новых и оценки существующих СФЗ, использует реальный план СФЗ без упрощений, легко справляется с масштабированием структуры СФЗ, генерирует сценарии атак автоматически в ходе испытаний. Она может использоваться для моделирования нескольких параллельных атак, для определения наиболее опасных направлений атак и уязвимых траекторий, а также менять тип угроз и модели нарушителей при исследовании уязвимости.

Список литературы

1. Wely I.Ch.E., Chetaine A. Analysis of physical protection system effectiveness of nuclear power plants based on performance approach. Annals of Nuclear Energy, 2021, vol. 152, art. 107980. doi: 10.1016/j.anucene.2020.107980.

2. Jiwei Z., Shunlong J., Jian L., Zhang L., Huaping C., Xiaofeng L. Optimization of communication probability in effectiveness evaluation of physical protection system. IEEE Access, 2020, vol. 8, pp. 228199–228205. doi: 10.1109/ACCESS.2020.3046037.

3. Тарасов А.Д., Шрейдер М.Ю., Боровский А.С. Метод проектирования систем физической защиты на основе генетического алгоритма // Интеллект. Инновации. Инвестиции. 2017. № 9. С. 70–74.

4. Chen S., Xiang D., Jin B., Jin H. Vulnerability assessment for physical protection systems of cave temples: A fuzzy petri net approach. Heliyon, 2024, vol. 10, no. 12, art. e33100. doi: 10.1016/j.heliyon.2024.e33100.

5. Kostin V., Borovsky A. Definition of basic violators for critically important objects using the information probability method and cluster analysis. CEUR Workshop Proc. Proc. ITNT, 2020, vol. 2667, pp. 343–347.

6. Шнякина Е.А., Костин В.Н. Разработка алгоритмического обеспечения принятия решений по идентификации типовых нарушителей категорируемым объектам // Изв. высших учебных заведений. Поволжский регион. Технич. науки. 2023. № 3. С. 72–82. doi: 10.21685/2072-3059-2023-3-5.

7. Костин В.Н. Методика формирования элементов структуры организационного управления систем физической защиты на основе информационного подхода // Тр. ИСА РАН. 2020. Т. 70. № 1. С. 30–39. doi: 10.14357/20790279200104.

8. Čakija D., Ban Ž., Golub M., Čakija D. Optimizing physical protection system using domain experienced exploration method. Automatika, 2020, vol. 61, no. 2, pp. 207–218. doi: 10.1080/00051144.2019.1698192.

9. Setiawan Y.A., Chirayath S.S., Kitcher E.D. MAPPS: A stochastic computational tool for multi-path analysis of physical protection systems. Annals of Nuclear Energy, 2020, vol. 137, art. 107074. doi: 10.1016/j.anucene.2019.107074.

10. Yang J., Huang L., Ma H. et al. A 2D-graph model-based heuristic approach to visual backtracking security vulnerabilities in physical protection systems. IJCIP, 2022, vol. 38, art. 100554. doi: 10.1016/j.ijcip.2022.100554.

11. Гаврилов П.М., Слюсарев А.В., Момот А.И. и др. Способ оценки эффективности системы физической защиты важного государственного объекта: Свид. о регистр. ПрЭВМ № 2724909C1. Рос. Федерация, 2020.

12. Жилин Р.А., Мельников А.В., Щербакова И.В. К вопросу о модели нарушителя системы безопасности объекта охраны // Вестн. Воронежского института МВД России. 2019. № 2. С. 57–69.

13. Шарков И.К. Имитационное моделирование средств физической защиты на охраняемом объекте в задачах оценки уязвимости // ИМСВН-2020: тр. конф. 2020. С. 254–264.

14. Шарков И.К., Желудков Е.А. Применимость эвристического алгоритма для задач поиска траекторий движения через систему физической защиты // SEIM-2019: сб. тр. конф. 2019. Т. 2. С. 34–40.

15. Костин В.Н. Оценка эффективности физической защиты информации критически важных объектов на основе марковских цепей // Информационные технологии. 2019. Т. 25. № 12. С. 757–765. doi: 10.17587/it.25.757-765.

16. Zou B., Li M., Yang M. Vulnerability learning of adversary paths in Physical Protection Systems using AMC/EASI. Progress in Nuclear Energy, 2021, vol. 134, art. 103666. doi: 10.1016/j.pnucene.2021.103666.

17. Zou B., Wang W., Liu J. et al. Development of a structure analytic hierarchy approach for the evaluation of the physical protection system effectiveness. Nuclear Engineering and Technology, 2020, vol. 52, no. 8, pp. 1661–1668. doi: 10.1016/j.net.2020.01.033.

Software & Systems doi: 10.15827/0236-235X.149.077-088 2025, 38(1), pp. 77–88

Simulation modeling of physical protection systems in AKIM environment

Yury B. Senichenkov [1], **Ilya K. Sharkov** [1]

[1] Peter the Great SPbPU, St. Petersburg, 195251, Russian Federation
[2] The PENTACON Company, St. Petersburg, 197198, Russian Federation

For citation
Senichenkov, Yu.B., Sharkov, I.K. (2025) ‘Simulation modeling of physical protection systems in AKIM environment’, *Software & Systems*, 38(1), pp. 77–88 (in Russ.). doi: 10.15827/0236-235X.149.077-088
Article info
Received: 02.05.2024 After revision: 23.07.2024 Accepted: 13.08.2024

Abstract. The paper discusses the methodology of building simulation models in the domestic software package AKIM. The models focus on solving the problem of analyzing the security level of existing and designed systems of physical protection of objects. They also use statistical experiment to form estimates of such systems’ effectiveness. The authors give a review of existing modern approaches to solving a similar problem. Most approaches apply Markov chains to search for vulnerable paths, as well as attack and defense graphs to assess the system effectiveness. Alternatively, it is suggested to build a simulation model without building an attack and defense graph, relying only on a physical defense system plan. The model in the AKIM environment consists of base class instances that model real elements of a physical protection system. As a result, there is a plan for models of agents and guards to move, simulating real attacks. The approach allows describing in detail the functions, reactions and capabilities of the system at the level of its elements and specifying the actual parameters of intruders and guards. This ensures accuracy and completeness of the analysis without simplification or exclusion of important details. Demonstration examples show that efficiency estimates of system protection models obtained by AKIM software package are close to efficiency estimates of system models built using Markov chains. In this case, the considered method of building simulation models allows overcoming the difficulties associated with using Markov chains: the need to use expert estimates of the coefficients of the transition matrix, large size matrices, the complexity of model modification.
Keywords: simulation modeling, physical protection system, agent-based modeling, Markov chains, performance evaluation, intruder attack, path finding algorithms
Acknowledgements. The author expresses his deep gratitude and appreciation to his supervisor Yury Borisovich Senichenkov, Doctor of Technical Sciences, co-author, who passed away in October 2024

References

1. Wely, I.Ch.E., Chetaine, A. (2021) ‘Analysis of physical protection system effectiveness of nuclear power plants based on performance approach’, *Annals of Nuclear Energy*, 152, art. 107980. doi: 10.1016/j.anucene.2020.107980.

2. Jiwei, Z., Shunlong, J., Jian, L., Zhang, L., Huaping, C., Xiaofeng, L. (2020) ‘Optimization of communication probability in effectiveness evaluation of physical protection system’, *IEEE Access*, 8, pp. 228199–228205. doi: 10.1109/ACCESS.2020.3046037.

3. Tarasov, A.D., Shrader, M.Yu., Borovskiy, A.S. (2017) ‘Design method for physical protection systems based on the genetic algorithm’, *Intellect. Innovations. Investments*, (9), pp. 70–74 (in Russ.).

4. Chen, S., Xiang, D., Jin, B., Jin, H. (2024) ‘Vulnerability assessment for physical protection systems of cave temples: A fuzzy petri net approach’, *Heliyon*, 10(12), art. e33100. doi: 10.1016/j.heliyon.2024.e33100.

5. Kostin, V., Borovsky, A. (2020) ‘Definition of basic violators for critically important objects using the information probability method and cluster analysis’, *CEUR Workshop Proc. Proc. ITNT*, 2667, pp. 343–347.

6. Shnyakina, E.A., Kostin, V.N. (2023) ‘Development of algorithmic support for decision-making to identify typical violators of categorized objects’, *University Proc. Volga Region. Tech. Sci.*, (3), pp. 72–82 (in Russ.). doi: 10.21685/2072-3059-2023-3-5.

7. Kostin, V.N. (2020) ‘Formation technique of elements of the structure of organizational management of physical protection systems based on the information approach’, *Proc. ISA RAS*, 70(1), pp. 30–39 (in Russ.). doi: 10.14357/20790279200104.

8. Čakija, D., Ban, Ž., Golub, M., Čakija, D. (2020) ‘Optimizing physical protection system using domain experienced exploration method’, *Automatika*, 61(2), pp. 207–218. doi: 10.1080/00051144.2019.1698192.

9. Setiawan, Y.A., Chirayath, S.S., Kitcher, E.D. (2020) ‘MAPPS: A stochastic computational tool for multi-path analysis of physical protection systems’, *Annals of Nuclear Energy*, 137, art. 107074. doi: 10.1016/j.anucene.2019.107074.

10. Yang, J., Huang, L., Ma, H. et al. (2022) ‘A 2D-graph model-based heuristic approach to visual backtracking security vulnerabilities in physical protection systems’, *IJCIP*, 38, art. 100554. doi: 10.1016/j.ijcip.2022.100554.

11. Gavrilov, P.M., Slyusarev, A.V., Momot, A.I. et al. (2020) *Method for Assessing the Effectiveness of the Physical Protection System of an Important State Object*, Pat. RF, № 2724909C1.

12. Zhilin, R.A., Melnikov, A.V., Shcherbakova, I.V. (2019) ‘To the question of the intruder model of the security system of the security object’, *Bull. of the Voronezh Institute of the Ministry of Internal Affairs of Russia*, (2), pp. 57–69 (in Russ.).

13. Sharkov, I.K. (2020) ‘Simulation modeling of physical protection systems in the tasks of vulnerability assessment’, *Proc. IMSVN-2020*, pp. 254–264 (in Russ.).

14. Sharkov, I.K., Zheludkov, E.A. (2019) ‘Applicability of heuristic algorithm for tasks of search of movement trajectories through physical protection system’, *Proc. SEIM-2019*, 2, pp. 34–40 (in Russ.).

15. Kostin, V.N. (2019) ‘Assessment of efficiency of physical security of information of crucial objects on the basis of Markov chains’, *Information Tech*., 25(12), pp. 757–765 (in Russ.). doi: 10.17587/it.25.757-765.

16. Zou, B., Li, M., Yang, M. (2021) ‘Vulnerability learning of adversary paths in Physical Protection Systems using AMC/EASI’, *Progress in Nuclear Energy*, 134, art. 103666. doi: 10.1016/j.pnucene.2021.103666.

17. Zou, B., Wang, W., Liu, J. et al. (2020) ‘Development of a structure analytic hierarchy approach for the evaluation of the physical protection system effectiveness’, *Nuclear Engineering and Technology*, 52(8), pp. 1661–1668. doi: 10.1016/j.net.2020.01.033.

Авторы

Сениченков Юрий Борисович [1], д.т.н., доцент, профессор, senyb@mail.ru

Шарков Илья Кириллович [1], исследователь, ведущий разработчик, shark2.1@mail.ru

[1] Санкт-Петербургский политехнический университет Петра Великого, г. Санкт-Петербург, 195251, Россия

[2] Компания ПЕНТАКОН, г. Санкт-Петербург, 197198, Россия

Authors

Yury B. Senichenkov [1], Dr.Sci. (Engineering), Associate Professor, Professor, senyb@mail.ru

Ilya K. Sharkov [1], Researcher, Leading Developer, shark2.1@mail.ru

[1] Peter the Great SPbPU, St. Petersburg, 195251, Russian Federation

[2] The PENTACON Company, St. Petersburg, 197198, Russian Federation