УКД 519.87 + 004.056

Булатов Д. К., Соколов А. Н.

ПРИМЕНЕНИЕ АЛГОРИТМА ВОЛНОВОЙ ТРАССИРОВКИ В ЗАДАЧАХ МОДЕЛИРОВАНИЯ ИНЖЕНЕРНО-ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

Рассмотрен алгоритм волновой трассировки применительно к задачам, связанным с моделированием физической безопасности объекта как элемента инженерно-технической защиты информации. Описаны этапы работы алгоритма волновой трассировки и условия его применения в рассматриваемых задачах. Уточнен спектр решаемых задач. Проведен сравнительный анализ алгоритма с традиционно применяемыми графовыми алгоритмами и алгоритмами, основанными на поиске глобального минимума функционала. Проанализированы возможности развития и комплексного применения моделей информационной безопасности, построенных на основе алгоритма волновой трассировки.

Ключевые слова: *алгоритм волновой трассировки, графовый алгоритм, алгоритм поиска глобального минимума функционала, инженерно-техническая защита информации, информационная безопасность, физическая безопасность.*

Bulatov D. K., Sokolov A. N.

APPLYING THE ALGORITHM WAVE TRACE FOR MODELING TECHNICAL PROTECTION OF INFORMATION

The algorithm of the wave trace applied to the problems associated with modeling the physical security of the object as an element of technical protection of information. The stages of the algorithm wave tracing and conditions for its use in these problems. Clarified range of tasks. Carried out a comparative analysis of the algorithm with the traditionally used graph algorithms and algorithms based on finding the global minimum of the functional. The possibilities of development and comprehensive application of information security models that are based on the wave tracing algorithm.

Keywords: *wave tracing algorithm, graph algorithm, the algorithm search for the global minimum of the functional, technical information security, information security, physical security.*

Ввиду разнообразия и уникальности каждого объекта информатизации, информационной системы и, в общем случае, каждого информационного ресурса, проектирование системы защиты является сложным процессом, в котором преимущественно применяются экспертные знания, опыт специалистов при проектировании систем инженерно-технической защиты информации[1]. Поэтому моделирование процессов, объектов, информационных систем является важным аспектом обеспечения информационной безопасности. Однако необходимым условием обеспечения комплексной защиты информации является создание определенных критериев, позволяющих оценить защищенность и определить достаточность мер, предпринятых для защиты от угроз. Именно моделирование позволяет унифицировать систему защиты и установить критерии оценки (показатели) защищенности объекта. Непосредственный интерес представляют математические модели, позволяющие на основании выбранных критериев оценить систему защиты объекта на соответствие предъявляемым требованиям, – в частности, оценить физическую защищенность объекта[2] как элемент инженерно-технической защиты информации.

Основные задачи[3], которые ставятся при моделировании обеспечения физической безопасности объекта:

1) оценка эффективности систем безопасности;

2) оценка безопасности различных стратегий;

3) оптимизация систем безопасности, т. е. приведение в соответствие заданному критерию при минимальных расходах на их построение.

В задачах трассировки печатных плат и нахождении кратчайшего пути в двумерном лабиринте широко применяется алгоритм волновой трассировки[4] (волновой алгоритм, алгоритм Ли), основанный на поиске кратчайшего пути на планарном графе. Он принадлежит к алгоритмам, основанным на методах поиска в ширину. Применение его в задачах обеспечения информационной безопасности является новым.

Алгоритм волновой трассировки, как основа для моделирования физической защиты объекта, позволяет решать комплекс задач, связанных с локацией злоумышленника на объекте защиты. При этом множество реализуемых моделей предполагает рассмотрение физического передвижения злоумышленника по территории защищаемого объекта. В зависимости от реализации алгоритма возможна оценка:

1) нарушителя (внутреннего и внешнего);

2) стихийного бедствия (распространения пожара);

3) возможности размещения технических средств перехвата информации в границах периметра защищаемого объекта.

Классическое решение задачи основывается на алгоритмах нахождения кратчайшего пути в графах. Объект представляется совокупностью вершин, соответствующих элементам рубежей защиты, и ребер, характеризующих способность нарушителя переходить от одной вершины к другой с целью преступной акции. Ребрам (либо вершинам) присваивается определенный показатель, как, например, вероятность обнаружения на каждом рубеже, либо время задержки злоумышленника. Именно на таком графе решается задача нахождения кратчайшего пути. На основании значения пути оценивается надежность и эффективность системы защиты. Однако существенным недостатком такого метода является его избыточность при моделировании сложных объектов и учете всех возможных переходов злоумышленника от одного рубежа защиты к другому.

При моделировании физической защиты объекта маршрут злоумышленника (вне зависимости от его типа) обладает свойством последовательности: злоумышленник не может появиться «ниоткуда» на объекте защиты и исчезнуть в «никуда». Его маршрут непрерывен и в каждой точке характеризуется такими параметрами, как вероятность обнаружения и время задержки. Интегрированием этих параметров можно получить искомый показатель безопасности для системы с большей точностью, чем в графовом алгоритме. С другой стороны, рассматриваемый алгоритм является некоторым упрощением алгоритма, основанного на поиске глобального минимума функционала.

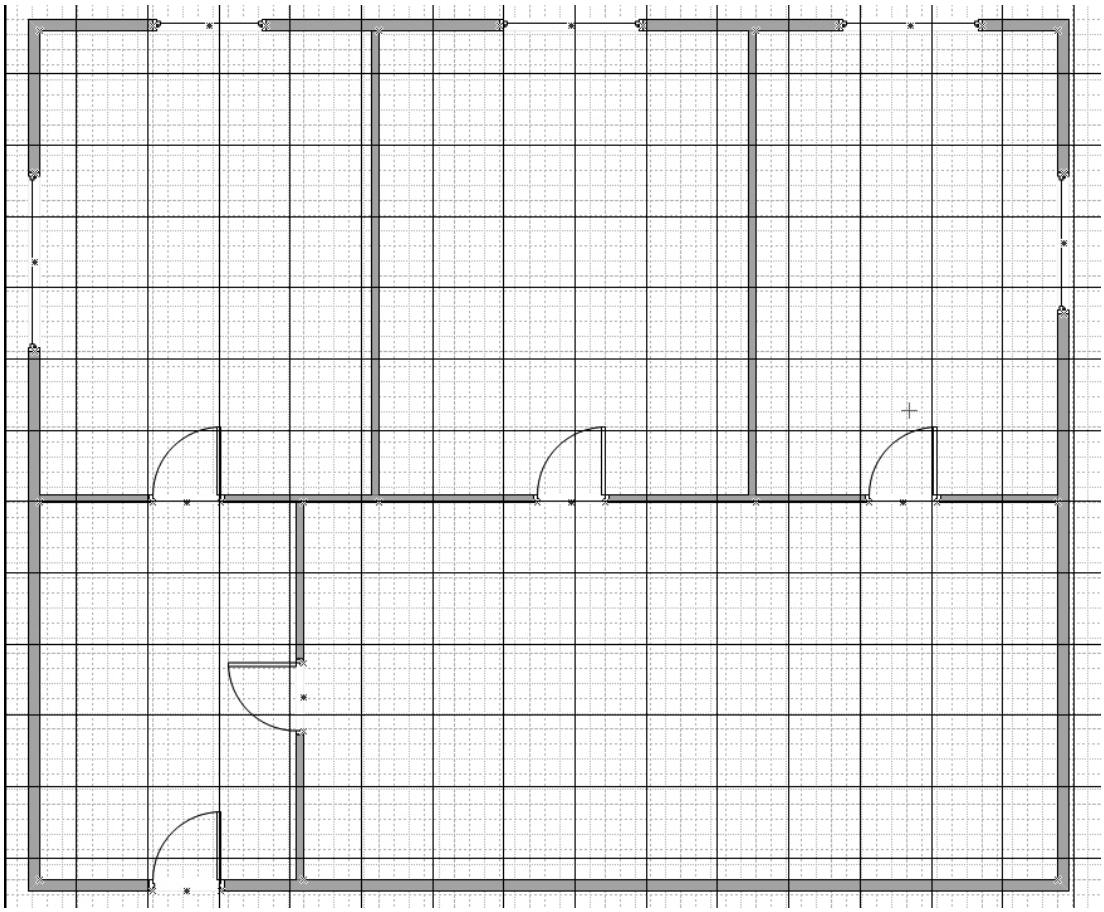

Рис. 1. План объекта с разбиением на ячейки

Алгоритм волновой трассировки реализуется в три этапа:

1) инициализация;
2) распространение волны;
3) восстановление пути.

На первом этапе объект, представленный в виде плана или схемы, разбивается на ячейки, размер которых должен обеспечивать различимость элементов инженерных конструкций и средств защиты (рис. 1).

С учетом разбиения создаются маски объекта:

1) маска физической доступности элементов объекта, которая характеризует физический маршрут злоумышленника, его возможность либо невозможность преодоления физических ограждений, а также характер преграждающих конструкций: дверей, окон, турникетов и т. д.;

2) маска системы безопасности, которая задает для каждой ячейки параметры вероятности фиксации либо обнаружения злоумышленника.

В общем случае применения алгоритма волновой трассировки достаточно двух масок, но модель может быть расширена путем добавления новых, например, маски огнеустойчивости среды, маски зон возможного снятия ПЭМИН, маски акустической разведки и т. д. На первом этапе также выбираются ячейки цели и исходные ячейки выдвижения злоумышленника.

Второй этап включает непосредственную реализацию волнового метода: на каждом шаге алгоритма рассчитывается новый фронт волны, то есть множество ячеек, в которые может переместиться злоумышленник из множества ячеек предыдущего шага (рис. 2). При этом происходит расчет параметров по маскам в зависимости от искомого параметра моделирования.

В ситуации, когда нас интересует исключительно параметр системы, как, например, показатель вероятности обнаружения на наиболее оптимальном маршруте, либо минимальная вероятность обнаружения, алгоритм может закончить свою работу.

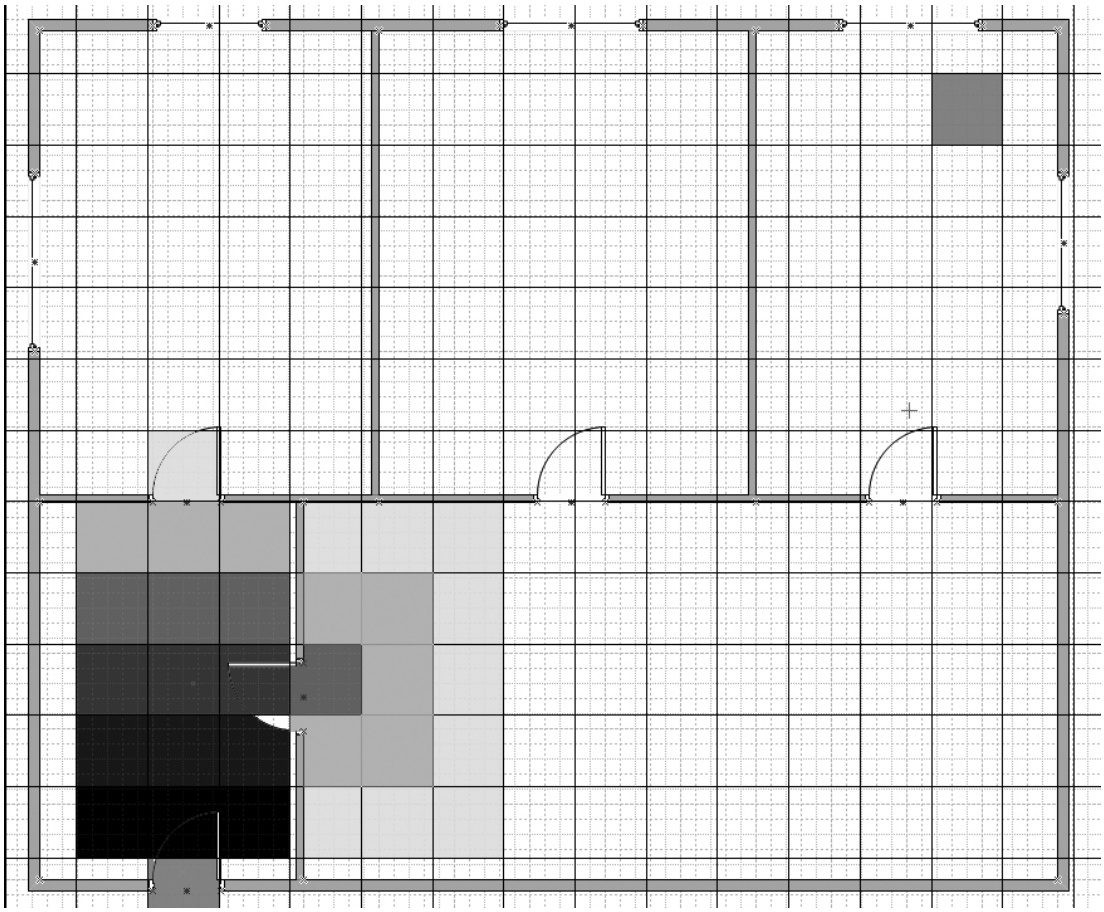

Рис. 2. Распространение фронта волны

Третий этап предполагает восстановление пути злоумышленника: методом обратного прохода от ячейки цели нарушителя восстанавливается маршрут, обусловленный заданными параметрами.

Алгоритм волновой трассировки используется в моделях, занимающих промежуточное положение между классическими графовыми моделями и моделями, основанными на поиске глобального минимума функционала, и обладает определенными преимуществами:

1) по сравнению с графовыми алгоритмами позволяет получить более точные результаты моделирования и использует более простую систему исходных данных;

2) по сравнению с алгоритмами, основанными на поиске глобального минимума функционала, более прост в реализации.

Рассмотренный алгоритм имеет высокий потенциал применения при моделировании различных аспектов обеспечения информационной безопасности.

Примечания

[1] Инженерно-техническая защита информации [текст]/А.А. Торокин. – М.: Гелиос АРВ, 2005. – 958 с.

[2] Проектирование и оценка систем физической защиты [текст]/ М.Гарсиа. – М.: Мир, 2003. – 386 с.

[3] Математические модели безопасности [текст]/ Вл. Вит. Башуров, Т. И. Филимоненкова. – Новосибирск: Наука, 2009 – 87 с.

[4] Графы в программировании: обработка, визуализация и применение [текст]/ В. Н. Касьянов, В. А. Евстигнеев – СПб.: БХВ-Петербург, 2003. – 1104 с.

References

[1] Engineering and Technical Information Security [text]/A.A. Torokin. – Moscow: Gelios ARV Publ., 2005. – 958 p. (In Russ.)

[2] Design and Assessment of the Systems of Physical Security [text]/ M.Garsia. – Moscow: Mir Publ., 2003. – 386 p. (In Russ.)

[3] Mathematical Models of Security [text]/ Vl.Vit. Bashurov, T.I. Filimonenkova. – Novosibirsk: Nauka Publ., 2009 – 87 p. (In Russ.)

[4] Graphs in Programming: Processing, Visualization, and Application [text]/ V.N. Kas'yanov, V.A. Evstigneev – St. Petersburg: BKhV-Peterburg Publ., 2003. – 1104 p.

Булатов Данил Кабирович, студент кафедры безопасности информационных систем ФГБОУ ВПО «Южно-Уральский государственный университет» (национальный исследовательский университет). E-mail: DANILDAZ@mail.ru

Соколов Александр Николаевич, кандидат технических наук, доцент, зав. кафедрой безопасности информационных систем ФГБОУ ВПО «Южно-Уральский государственный университет» (национальный исследовательский университет). E-mail: ANSokolov@inbox.ru

Danil Kabirovich Bulatov, student of the Department of Information System Security of the Federal State Budgetary Educational Institution of Higher Professional Education 'South Ural State University'. E-mail: DANILDAZ@mail.ru

Sokolov Aleksandr Nikolaevich, candidate if engineering sciences, associate professor, head of Information Systems Security Department, South Ural State University (national research university). E-mail: ANSokolov@inbox.ru