УДК 654.949

Поддержка принятия решений при управлении системой безопасности территориально распределенного объекта

С.С. Звежинский, А.И. Ларин, В.А. Передня

Новый метод имитационного моделирования угроз основан на представлении пространственно распределенного объекта как суперпозиции кулоновских потенциалов «притяжения» - возможных целей нарушителя и потенциалов «отталкивания» - от мест размещения технических средств физической защиты, сил охраны и других значимых для моделирования сущностей. Показана непротиворечивость результатов моделирования в среде MathLab и ГИС-технологий для основных типов нарушителей.

Введение

Моделирование угроз безопасности территориально-распределенным объектам является важным научно-методическим инструментом по оценке эффективности их защищенности и выработки рациональных управленческих решений силам охраны. Для этого в большинстве случаев применяются «табличные» или методы имитационного моделирования, основанные на установлении четкого соответствия множеств: источники угроз - потенциальные цели (уязвимости) - технические средства физической защиты (ТСФЗ) и силы охраны. Большинство таких имитационных моделей основаны на вероятностно-временном анализе (расчете) соответствующих матриц в конкурирующей системе «нарушитель / силы охраны», - сравнении времен вероятного продвижения противоборствующих сторон к уязвимым целям (точкам) объекта. К ним относятся модель и соответствующее специальное программное обеспечение (СПО) EASI (США), применяемая для оценки угроз по определенным сценариям вторжения, и аналогичное отечественное СПО «Вега-2» («СНПО «Элерон», г. Москва). Сравнительный анализ расчетных матриц позволяет выявить наиболее уязвимые места объекта, перераспределить силы охраны, выдать рекомендации по применению дополнительных ТСФЗ и пр. [1, 2].

К общим недостаткам таких СПО можно отнести невозможность оценки угроз объекту без сигнализационных ТСФЗ, ненаглядность и недостаточная адекватность результатов для территориально-распределенных объектов (например, вследствие игнорирования географической информации), невозможность прогнозирования вероятных (недетерминированных) путей движения нарушителя. Это дает основание для развития других методов, в определенной степени преодолевающих указанные недостатки. Недавно был предложен метод имитационного моделирования, основанный на новом представлении и оценке угроз территориально-распределенным объектам с использованием технологии современных геоинформационных систем (ГИС) [3]. Данная работа посвящена развитию феноменологии и алгоритмам реализации этого метода.

Феноменологические основы метода моделирования

Возможный путь вторжения и перемещения по территории

пространственно-распределенного объекта является сложным процессом, спрогнозировать который позволяет то, что нарушитель, как правило, реализует две главные стратегии поведения (другие модели – промежуточные): 1) достижение цели (выявленной или существующей уязвимости) с наибольшей вероятностью или наименьшем сопротивлении силам охраны и наименьшей возможностью быть обнаруженным; 2) минимизация времени прохождения пути (быстрее, чем охрана отреагирует), не считаясь с возможным обнаружением ТСФЗ и другими условиями, например, климатикой, которая в определенной степени влияет на маршрут.

Известно, что современные ГИС-технологии (цифровые карты местности и др.) позволяют учитывать природно-климатические и физико-географические условия (ФГУ) местности, которые влияют на выбор маршрута перемещения различных нарушителей. Кроме того, т.н. «гравитационные» модели влияния антропогенных факторов, применяемые в экономике и социологии, достаточно корректно описывают, например, влияние миграционных факторов, действие которых находится в обратной зависимости от расстояния до источников [4]. Это позволяет сформировать феноменологическую основу нового метода имитационного моделирования.

Имитационная модель угроз

В основу имитационной модели положено описание объекта охраны как искусственно сформированного «электростатического» поля потенциалов, созданных двумя типами точечных зарядов $\boldsymbol{Q_i}$, имеющих противоположные знаки, а нарушитель в виде единичного положительного заряда $+\boldsymbol{q}$, который перемещается по этому полю в соответствии с двумя вышеназванными стратегиями. «Точечные» источники потенциалов угроз размещаются:

- в местах расположения целей (уязвимости), создающих «притяжение» для нарушителя своими зарядами с отрицательным знаком $-\boldsymbol{Q_k}$;
- в местах размещения сил охраны и ТСФЗ, а также значимого действия ФГУ, создающих потенциал «отталкивания» зарядами $+\boldsymbol{Q_m}$; $\boldsymbol{i = k+m}$.

Величины Q_k, $k = 1,...p$ определяются (в общем случае экспертными методами) в соответствие с ущербом, который нарушитель может нанести в этом месте (уязвимости). Величины Q_m, $m = 1,...s$ определяются (также экспертным образом) в соответствии с относительной «силой» противодействия нарушителю. Заметим, что как ток течёт путём наименьшего сопротивления, также и нарушитель для выбранной тактики передвигается путем, позволяющим с наименьшими «затратами» достичь цели.

Экспертные оценки величин (весов) кулоновских зарядов Q_k, Q_m должны соответствовать выбранной обобщенной модели нарушителя, то есть для различных типов нарушителей – они различные. Для их получения целесообразным видится использование экспертного метода анализа иерархий Саати с парными сравнениями однотипных элементов [4]. Как показывает опыт, в абсолютном большинстве случаев достаточно ограничиться 4-я обобщенными типовыми моделями нарушителя [5]:

1) «случайный»;

2) «неподготовленный»;

3) «подготовленный»;

4) «осведомленный».

Случайный нарушитель – индивидуум, проникший на объект по незнанию, возможно не имеющий злого умысла (по глупости, невнимательности и пр.), однако обладает возможностью нанесения ущерба. Неподготовленный нарушитель – человек, у которого в намерении принести какой-либо ущерб объекту охраны, но не имеющий навыков вторжения, кражи и другой противоправной деятельности. Подготовленный нарушитель – типично профессиональный мошенник, вор и пр., который готовится к вторжению и знает общие принципы построения систем физической защиты. Осведомлённый нарушитель – наиболее опасный тип, это профессионал, например террорист или диверсант, обладающий информацией о СФЗ объекта, ценностях, сотрудниках, возможно имеющий преступный сговор с сотрудником объекта.

Новизна феноменологического подхода к имитационному моделированию заключается в изменении «образа» объекта охраны - распределения зарядов Q_m, Q_k (как относительных весов, так и возможных мест их размещений); в известных моделях «объект» оставался неизменным, а изменялись модели действий нарушителя [1, 2, 5].

Кулоновский потенциал от точечного источника «притяжения» (цель нарушителя) или «отталкивания» (ТСФЗ, локальные ФГУ и пр.) имеет вид [6]:

$$\varphi = \frac{Q}{r},$$

и здесь возникает неопределенность при $r \to 0$. Поскольку реальный источник поля «притяжения» или «отталкивания» в территориально распределенном объекте охраны имеет некоторый физический размер, например R, то для задания потенциала в зоне (на площади) источника потенциал ограничивается, как для физического аналога заряженной сферы:

$$\varphi = \frac{Q}{r} \text{ при } r > R, \quad \varphi = \frac{Q}{R} \text{ при } r \le R. \qquad (1)$$

Скалярные потенциалы от источников $-\boldsymbol{Q_k}$ и $+\boldsymbol{Q_m}$, размещенные в соответствующих местах объекта, по принципу суперпозиции формируют искомое поле угроз или «теплокарту» скалярного потенциала:

$$\varphi_\Sigma(r) = \sum_{m=1}^{p} \varphi_m(r) + \sum_{k=1}^{s} \varphi_k(r) \ldots\ldots\ldots \qquad \ldots\ldots\ldots\ldots\ldots\ldots (2)$$

Термин «теплокарта» выбран по аналогии с радужно расцвечиваемым тепловизионным изображением, где зеленый цвет характеризует условно среднюю температуру фона, красный – положительный контраст относительно фона, а синий – отрицательный контраст температуры. Таким образом, синий цвет теплокарты угроз характеризует впадины (потенциальные ямы) в местах сосредоточения целей нарушителей и преимущественного их перемещения. Красный цвет характеризует места размещения ТСФЗ, сил охраны и пр. – то есть тех мест, которые нарушитель будет, по возможности, избегать.

Кроме того, возможное направление перемещение нарушителя (единичного положительного заряда $\boldsymbol{q}$) по «теплокарте» в первом приближении может рассматриваться в направлении действия градиента потенциала $\varphi_\Sigma(r)$ в заданной точке, физический аналог – вектор напряженности поля $\vec{E}$ [6].

Определив вектор $\vec{E}$ в точках территориально распределенного объекта, возможно наглядно представить вероятную траекторию движения нарушителя, помещенного первоначально на границе объекта, к выделенным целям, в соответствии с:

$$\vec{E} = -grad\ \frac{\partial \varphi_{\in}}{\partial r}. \quad (3)$$

Необходимо отметить, что адекватность распределения теплокарты угроз и траекторий вероятного перемещения нарушителя по объекту для данного метода напрямую зависит от точности и квалификации группы экспертов, которая должна не только разместить на цифровой карте объекте *p* целей нарушителя (уязвимых мест) и *s* точек «отталкивания» (ТСФЗ, силы охраны и пр.), но и определить их условные веса.

Моделирование

Для имитационного моделирования по (1) - (3) было выбран прикладной пакет программ MathLab, которое встраивалось в типовое ГИС-приложение. В качестве последнего было выбрано QGIS (Швейцария) ввиду его бесплатности, широкого функционала, открытости кода и встроенной возможности создания модулей на языке программирования Python. QGIS обеспечивает возможность изменения исходного кода; основные модули автоматически входят в новую версию, оно позволяет работать с цифровыми картами различных форматов, выполнять послойно их анализ, масштабировать и пр.

Для оценки адекватности метода потенциалов, в качестве примера использовался файл *MO.qgs* с геоинформацией по Московской области; был выбран известный объект охраны (периметр более 5 км), находящийся в 40 км к юго-востоку от г. Москвы. Цифровая карта объекта была сохранена в файл **.qgs*; в слоях были выделены точки (зоны) «притяжения» и точки «отталкивания».

Экспертная группа в составе 9 человек (из них 2 д.т.н. и 4 к.т.н.) определяла относительные веса и расположения точек притяжения и отталкивания для четырех типов нарушителей. Были получены соответствующие теплокарты, характеризующие распределение потенциала угроз по объекту для различных типов нарушителей.

Выводы

Анализ результатов моделирования показал, что теплокарты угроз выбранному территориально распределенному объекту в первом приближении адекватно отображают предполагаемые действия типовых нарушителей с учетом их различной тактики. Однако прогнозирование вероятных траекторий перемещения нарушителя по (3) обладает меньшей адекватностью, но без потери логики.

В целом новый метод потенциалов для моделирования угроз пространственно-распределенным объектам имеет право на существование, обладает высокой наглядностью для быстрого принятия решений. Дальнейшие усилия будут направлены на его развитие, в том числе на снижение зависимости результатов от квалификации экспертной граппы, а также внесения динамических элементов в имитационную модель.

Список литературы

1. Петров, Н. Системы физической защиты // Н. Петров / - БДИ. - 2005. - № 3. – С.6-12.
2. Гарсиа, М. Проектирование и оценка СФЗ / М.Гарсиа. - М.: Мир, 2002. – 332 с.
3. Звежинский, С.С., Парфенцев, А.В., Передня, В.А. Моделирование пространственно распределенных угроз безопасности объектам посредством метода потенциалов // С.С. Звежинский, А.В. Парфенцев, В.А. Передня / Радиотехника. - 2016. - № 2. - С.41-43.
4. Теория систем и системный анализ в управлении организациями: Справочник / В.Н. Волкова [и др.]; под ред. В.Н. Волковой и А.А. Емельянова. – М.: Финансы и Статистика, 2006. – 848 с.
5. Звежинский, С.С., Иванов, В.А. Эффективность и результативность средств обнаружения // С.С. Звежинский, В.А. Иванов / БДИ. – 2005. - №5. – С. 64-70.
6. Трофимова, Т.И. Курс физики: учеб. пос. / Т.И. Трофимова. – М.: Академия, 2005. – 560 с.

Звежинский Станислав Сигизмундович – профессор кафедры «Информационная безопасность и автоматизация» Московского технического университета связи и информатики (МТУСИ), г. Москва, доктор технических наук, профессор, zwierz@rambler.ru;

Ларин Александр Иванович – доцент кафедры «Информационная безопасность и автоматизация» МТУСИ, кандидат технических наук, larin2004@list.ru;

Передня Вячеслав Александрович – аспирант МТУСИ, г. Москва; it@mtuci.ru.