ИПМ им.М.В.Келдыша РАН • Электронная библиотека

Препринты ИПМ • Препринт № 102 за 2019 г.

ISSN 2071-2898 (Print)
ISSN 2071-2901 (Online)

Балута В.И., Карандеев А.А., Сивакова Т.В.

Оценка антитеррористической защищенности объектов на основе расчета интегральных показателей

Рекомендуемая форма библиографической ссылки: Балута В.И., Карандеев А.А., Сивакова Т.В. Оценка антитеррористической защищенности объектов на основе расчета интегральных показателей // Препринты ИПМ им. М.В.Келдыша. 2019. № 102. 18 с. doi:10.20948/prepr-2019-102
URL: http://library.keldysh.ru/preprint.asp?id=2019-102

О р д е н а Л е н и н а
ИНСТИТУТ ПРИКЛАДНОЙ МАТЕМАТИКИ
имени М.В.Келдыша
Р о с с и й с к о й а к а д е м и и н а у к

В.И. Балута, А.А. Карандеев, Т.В. Сивакова

Оценка антитеррористической защищенности объектов на основе расчета интегральных показателей

Москва — 2019

Балута В.И., Карандеев А.А., Сивакова Т.В.

Оценка антитеррористической защищенности объектов на основе расчета интегральных показателей

В настоящей работе предлагается подход, позволяющий получить предварительную оценку эффективности системы защиты на основе использования небольшого числа входных параметров путем расчетного зонирования территории объекта. Предлагаемый расчетный метод может использоваться и для оптимизации размещения элементов системы с учетом имеющихся ограничений.

Ключевые слова: антитеррористическая безопасность, интегральный подход, защищенность объекта, зонирование

Victor Ivanovich Baluta, Alexander Andreevich Karandeev, Tatyana Vladimirovna Sivakova

Assessment of anti-terrorism security of objects based on the calculation of integrated indicators

In this paper, we propose an approach that allows us to obtain a preliminary assessment of the effectiveness of the protection system based on the use of a small number of input parameters by calculating the zoning of the object. The proposed calculation method can also be used to optimize the placement of system elements, taking into account the existing limitations.

Key words: anti-terrorism security, integrated approach, object security, zoning

Работа выполнена при поддержке Российского фонда фундаментальных исследований, проект № 16-29-09550 офи_м.

Введение

Актуальность вопросов совершенствования антитеррористической безопасности различного рода объектов в наше время остаётся весьма значимой. Нагнетание и эпизодическое усиление напряженности межгосударственных, межнациональных, межконфессиональных конфликтов создают почву для развития и активизации деятельности различного рода террористических организаций. Более того, такие организации используются политическими противниками в собственных интересах в рамках ведения информационных войн для дестабилизации обстановки, провоцирования роста напряжённости в обществе, а иногда – и устранения оппонентов. Возможность использования террористических актов в политических целях – основная причина, подпитывающая эти явления в современном мире. Хорошо известно, что объем средств, необходимых на подготовку и проведение терактов, на многие порядки меньше объема средств, требующихся для обеспечения всесторонней безопасности объектов.

Потенциально предметом террористической атаки могут стать самые разные объекты экономики, производства, инфраструктуры, социальной сферы, существенно различающиеся по своим характеристикам. Для решения организационных вопросов по обеспечению их защищённости выработан свод общих принципов и подходов, положенных в основу различных инструктивных документов. Как правило, основой оценок служат экспертные подходы (см., например, [1, 2]), в частности логико-вероятностные [3]. Однако конкретная их реализация зачастую приводит к неоднозначности. Так, в статье [4], одним из авторов которой является руководитель рабочей группы при Президенте РАН по анализу риска и проблем безопасности, научный руководитель многотомного (в 52 томах) издания «Безопасность России. Правовые, социально-экономические и научно-технические аспекты» А.Н. Махутов, отмечается, что в настоящее время «оформление паспортов безопасности опасных объектов и разработки планов их защищённости от угроз техногенного, природного характера и террористических актов основаны на использовании разнородных ведомственных методик. Численные значения выходных параметров данных методик, при прочих равных условиях, значительно различаются и не могут быть соотнесены с уровнем допустимого риска конкретного объекта». В указанной статье акцентируется также внимание на возрастании террористических угроз и обосновывается необходимость комплексного совершенствования подходов к обеспечению безопасности объектов, разработки единой методологии управления их безопасностью и создания систем поддержки принятия решений на интеллектуальной платформе, базирующейся на методах математического моделирования. Некоторые обобщенные взгляды на содержание и построение такой платформы предложены в работах [5, 6, 7].

Предлагаемый в данной работе подход расчётного зонирования области размещения средств защиты объекта и прилегающей к этой области территории рассматривается в качестве одного из инструментов такой платформы. Необходимость создания подобных инструментов обуславливается рядом особенностей проявления конфликтов террористической направленности. Акцентируем внимание на некоторых из них.

Прежде всего, понятно, что обеспечение антитеррористической безопасности объектов является специфической задачей управления, которая решается в условиях существенной неопределённости, при этом уровень и характер самой неопределённости не могут быть априори оценены достаточно достоверно, обычно нет данных даже о самой возможности нападения.

Другими словами, по своей содержательной сути конфликт между стороной нападения и стороной защиты существует преимущественно в виртуальном пространстве. Стороны конфликта большую часть времени находятся в состоянии предугадывания возможных действий друг друга, включая и прогнозирование ответных действий на собственные, то есть существенным, а зачастую и определяющим для достижения цели является оперирование в такого рода конфликтах рефлексиями высоких порядков. В задачах обеспечения безопасности противник, как правило, не присутствует явно, хотя субъект защиты постоянно предполагает его наличие, оперируя его виртуальным образом. Другими словами, субъект защиты большую часть времени находится в состоянии конфликта, как минимум, с гипотетическим субъектом нападения и в соответствии с этим осуществляет определённые действия по обеспечению безопасности объекта. Постоянный «бой с тенью», с точки зрения конфликтологии, является существенной особенностью предметной области комплексного обеспечения антитеррористической безопасности объектов.

Ещё одним важнейшим аспектом является скоротечность активной фазы событий, когда в ходе отражения террористической атаки практически отсутствует какая-либо возможность изменения планов и перестройки системы защиты. Поэтому, казалось бы, все возможные варианты развития событий должны быть проанализированы заранее и предусмотрены меры реагирования на них. В то же время очевидно, что в условиях существенной неопределённости все возможные варианты поведения противника и сценарии развития событий предусмотреть невозможно. Это означает, что стратегия защиты должна строиться на принципах одновременного учёта всего множества возможных вариантов.

Наличие большого объёма различного рода неопределённостей, актуализация которых имеет мультипликативный эффект, необходимость действовать эффективно в подобных условиях требуют развития специфических подходов к решению поставленной задачи – задачи обеспечения необходимого уровня безопасности объектов.

Условно уровни управления при решении задач обеспечения безопасности объектов можно разделить на стратегический, тактический и оперативный. Каждый из этих уровней отличается не просто горизонтом планирования, но и характером решаемых задач. Понятно, что задача *проектирования системы безопасности объекта* относится к задачам стратегического уровня, причём в ракурсе создания возможностей противодействия противнику при любом сценарии его действий. Технология интегрального подхода как нельзя лучше подходит для оценки качества проектных решений и их рационализации, в том числе при имеющихся ограничениях на ресурсы.

Описание алгоритма решения

Интегральный подход ориентирован на достаточно упрощённое оперативное определение ситуационных возможностей противостоящих сторон конфликтного взаимодействия. В рамках интегрального подхода содержание обстановки в модели описывается путём зонирования территории определённым образом с помощью специализированных вычислительных процедур. В качестве зон или их границ могут выступать такие аспекты задачи, как зона эффективного действия средств обнаружения нарушителя, граница перехвата нарушителя при входе на охраняемую территорию, возможная зона воздействия противника на объект охраны и т.д. Интегральные зоны могут быть рассчитаны автоматически на основании характеристик объектов и окружающей обстановки (динамических характеристик объекта нападения, характеристик средств обнаружения, рельефа местности, возможных препятствий для решения своих задач как той, так и другой стороной, и т.п.). По результатам расчёта возможно исследование полученных зон на предмет выявления их пересечений, объединений, дополнений и т.п. Последнее позволяет анализировать в обобщённом представлении как возможности системы обеспечения безопасности объекта, так и возможности противника по достижению его целей, другими словами, результаты анализа интерпретируются экспертами в контексте решения задачи определения ситуационных возможностей сторон конфликта.

Обобщённый пример решения задачи зонирования территории при организации системы защиты объекта от воздействия со стороны беспилотного летательного аппарата (БПЛА) приведён на рис.1.

Рис. 1. Пример размещения ключевых зон при оценке защищённости по интегральным показателям

На приведённом выше рис. 1 условно изображены следующие элементы обстановки:

- рельеф местности (в виде карты высот с цветовой гаммой от светло-зелёного до тёмно-коричневого цвета),
- защищаемый объект (в виде жёлтого круга, расположенного в низине),
- зона гарантированного воздействия противника на защищаемый объект при достижении им этой зоны (в виде тёмно-коричневого кольца вокруг жёлтого круга),
- технические средства обнаружения нарушителя (в виде белых треугольников),
- технические средства воздействия на нарушителя (в виде голубых кружков),
- граница зоны обнаружения (тёмно-зелёная область, окаймлённая белым контуром),
- граница зоны принятия решения о противодействии нарушителю (красный пунктир),
- граница зоны поражения нарушителя (красный контур).

Определение интегральных характеристик защищённости объекта осуществляется на основе результатов пространственно-временного анализа обстановки в окрестностях защищаемого объекта.

Алгоритм решения задачи построения соответствующих зон представляет собой последовательность выполнения следующей последовательности технологических процедур:

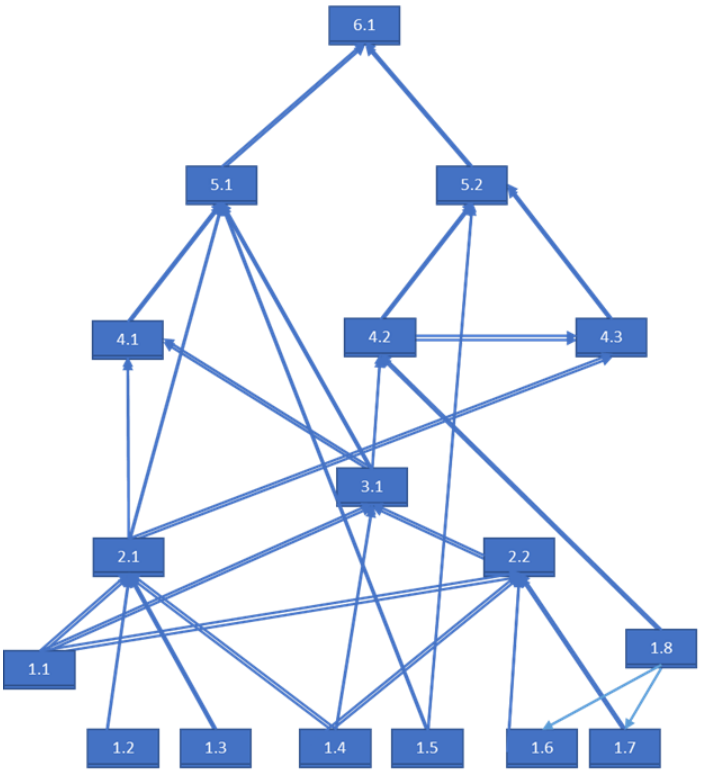
1. Формируется расчётная область решения задачи в виде трёхмерной модели пространства, включающей точку (зону) расположения защищаемого объекта и прилегающие к ней территории, на которой возможен процесс взаимодействия противостоящих сторон.

2. В расчётной зоне выделяется конфигурация и задаются характеристики защищаемого объекта, включая места вероятного интереса со стороны нарушителей (цели поражения).
3. На сформированную сцену наносятся места расположения средств обеспечения безопасности (средства обнаружения и средства поражения нападающих) и задаются их характеристики по решению целевых задач.
4. На основании данных о возможных средствах воздействия со стороны противника строится карта (граница) гарантированного поражения защищаемого объекта, исходя из предположения, что при достижении этой границы противник получает возможность нанесения ущерба объекту защиты.
5. На основании данных о сигнальных характеристиках противника рассчитывается граница зоны его обнаружения.
6. На основании данных о специфике системы управления силами и средствами обеспечения безопасности, предполагающей наличие интервала времени на обработку и идентификацию получаемых сигналов, выработку решений, доведение указаний до исполнителей, строится граница зоны принятия решения о формах воздействия на противника.
7. На основании динамических характеристик противника, полученной расчётным путём границы зоны его обнаружения и анализа регламентных ограничений по выработке решений системой управления, а также порядка действий сил реагирования определяется граница зоны поражения нарушителя – граница той зоны, которая может быть достигнута противником с учётом комплекса характеристик системы обеспечения безопасности объекта.
8. Анализируется взаимное расположение границ зоны гарантированного воздействия на объект и зоны поражения нарушителя. Их пересечение может указывать на наличие слабых мест в системе защиты объекта – наличие возможности для противника достичь точки, из которой он может нанести ущерб, используя бреши в системе обеспечения безопасности.

В ходе выполнения расчётов имеет смысл учитывать вероятностную природу рассчитываемых параметров, поскольку распределение их значений в пространстве неоднородно и зависит от ряда условий. Например, понятно, что эффективность средств обнаружения мало того что уменьшается с расстоянием, так ещё и зависит от множества факторов внешней среды – рельефа местности, погодных условий, времени суток, сигнальных характеристик нарушителя и др. Время на выработку решений системой управления тоже может варьироваться в каких-то пределах в зависимости от качества получаемых от систем обнаружения данных и их интерпретации. Это замечание о нечёткости данных касается и множества других параметров. В связи с чем расчёт соответствующих зон можно проводить либо в терминах консервативной схемы, когда используются только граничные значения параметров с

ориентацией на оценку нижнего уровня безопасности, что позволяет выстроить иерархию соответствующих зональных границ, либо в терминах формирования вероятностной картины, позволяющей получать более взвешенную картину для выработки стратегических решений.

Представление описанной последовательности действий в виде алгоритмической диаграммы приведено на прилагаемой схеме (рис. 2).



обозначения	
1.1	Рельеф
Цель	
1.2	характеристики
1.3	местоположение
Нарушитель	
1.4	характеристики
1.5	информированность
Средства обнаружения	
1.6	характеристики
1.7	местоположение
1.8	управление
Зоны	
2.1	досягаемости
2.2	обнаружения
3.1	позиции
4.1	скрытного проникновения
4.2	беспрепятственного движения
4.3	неконтролируемого воздействия
Защищенность	
5.1	от скрытного
5.2	от открытого
6.1	интегральная

Рис. 2. Диаграмма расчёта интегральных характеристик

Рассмотрим на гипотетическом примере реализацию описанного выше алгоритма.

Применение методики определения интегральных показателей

Исходные данные. Поскольку в предлагаемом примере в качестве исходных данных используются условные модельные представления для ниже обозначенных сущностей, их конкретная реализация не представляется существенной и не рассматривается:

- модель местности,
- характеристики цели (объекта защиты),
- местоположение цели,
- степень информированности нарушителя,
- характеристики нарушителя,

- характеристики средств обнаружения,
- расположение средств обнаружения,
- характеристики системы управления.

Модель местности – это пространственная модель препятствий для перемещения и воздействия в границах, в которых возможна реализация нападения на объект. В рассматриваемом примере используется «плоская» модель местности с множеством препятствий, которая отображена на приведённом ниже рисунке (рис. 3). На рисунке более светлым тоном обозначены зоны, непреодолимые при перемещении и при воздействии (например, здания, сооружения и т.п.).

Характеристики цели (в примере) – это совокупность тех характеристик, которые совместно с характеристиками средств воздействия позволяют рассчитать пространственные границы, воздействие из которых гарантированно переводит объект воздействия в состояние поражения (что и является целью террориста).

Местоположение цели – часть пространства, занимаемая целевым объектом. В расчётном примере объект нападения рассматривается как точечный относительно общего пространства территории взаимодействия субъектов защиты и нападения.

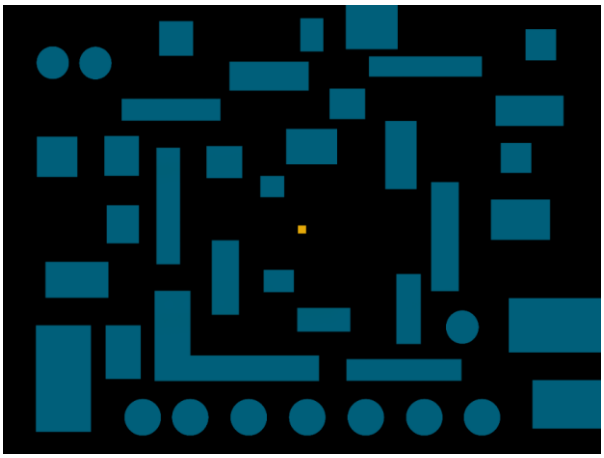


Рис. 3. Модель местности

Местоположение цели отмечено на исходной схеме (рис. 3) желтой квадратной меткой.

Информированность нарушителя – интегральная характеристика, отражающая достоверность и полноту всей информации об обстановке, которую нарушитель использует при планировании нападения. В рассматриваемом примере для простоты иллюстрации информированность нарушителя учитывается только в части, касающейся конфигурации поля обнаружения. Полная информированность о конфигурации поля обнаружения даёт нарушителю возможность поиска кратчайшего пути к цели.

Характеристики нарушителя (здесь) – это совокупность параметров, определяющих характер и скорость перемещения нарушителя по определенным участкам, в том числе возможности и затраты времени на преодоление различных препятствий, вероятности его обнаружения определенными средствами обнаружения в определенной обстановке, возможности нарушителя по воздействию на целевой объект.

Характеристики средств обнаружения – вероятность обнаружения определённого нарушителя (обладающего некоторым набором сигнальных характеристик) в определенных условиях обстановки (на определенном расстоянии, на определенном фоне, в определенной «помеховой» обстановке и т.п.), в том числе с учетом выбранного режима функционирования средств обнаружения.

Размещение средств обнаружения – точки в пространстве, представляющие координаты нахождения соответствующих элементов системы обнаружения.

Характеристики системы управления – это время на анализ обстановки и выработку системой управления решения по нейтрализации нарушителя определенного типа в определенной ситуации.

Пространственные расчеты. Пространственные расчеты включают:

- определение конфигурации и характеристик зоны досягаемости цели,
- определение конфигурации и характеристик поля обнаружения,
- определение ближайшей исходной позиции нарушителя,
- определение зоны скрытного воздействия на целевой объект,
- определение зоны беспрепятственного проникновения в зону обнаружения,
- определение зоны неконтролируемого воздействия на целевой объект.

Ниже рассматриваются результаты вычислений с учетом заданных в условном примере характеристик объектов и конфигурации препятствий.

Расчет конфигурации зоны досягаемости цели. Как представлено на схеме рис. 2, зона досягаемости цели рассчитывается на базе следующих исходных данных:

- характеристики цели;
- размещение цели,
- модель местности,
- характеристики нарушителя.

На основании боевых характеристик имеющихся у нарушителя средств нападения и защитных характеристик цели определяется зависимость вероятности поражения цели нарушителем от расстояния до цели. Конфигурация зоны досягаемости рассчитывается с использованием полученных характеристик вероятности поражения цели в зависимости от расстояния до нее и доступности цели для применяемых средств поражения, определяемой по местоположению цели и модели местности.

Пример расчета зоны досягаемости на основании некоторых гипотетических характеристик нарушителя и цели приведён на рис. 4, где показан результат расчета зоны воздействия на целевой объект со стороны нарушителя. Для простоты принято, что поражение возможно с некоторого расстояния при наличии прямой видимости объекта. Градациями светлых тонов обозначено повышение значений показателя: чем светлее – тем вероятность поражения цели выше. Обозначим эту зону как Z_{goal}.

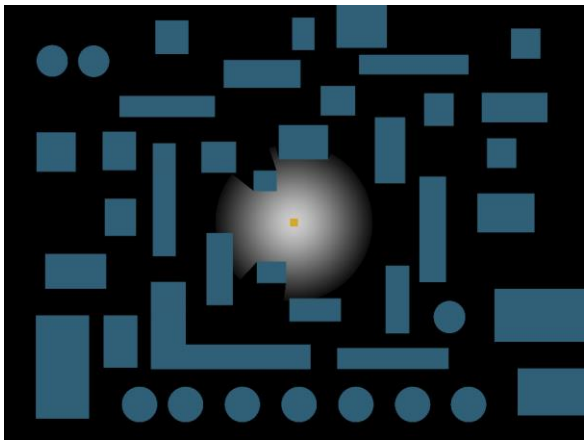


Рис. 4. Конфигурация зоны досягаемости цели Z_{goal}

Расчет конфигурации поля обнаружения. Под полем обнаружения будем понимать часть пространства, в любой точке которого вероятность обнаружения нарушителя имеющимися в системе обеспечения безопасности средствами отлична от нуля. При построении этого поля используются данные о размещении и характеристиках средств обнаружения, а также о сигнальных характеристиках нарушителя.

Пример построения поля обнаружения показан на рис. 5, где результаты расчёта также приведены в градациях серого цвета: чем светлее – тем выше вероятность обнаружения. Использовавшиеся в расчёте рабочие элементы системы обнаружения отображены на схеме зелёными квадратными метками.

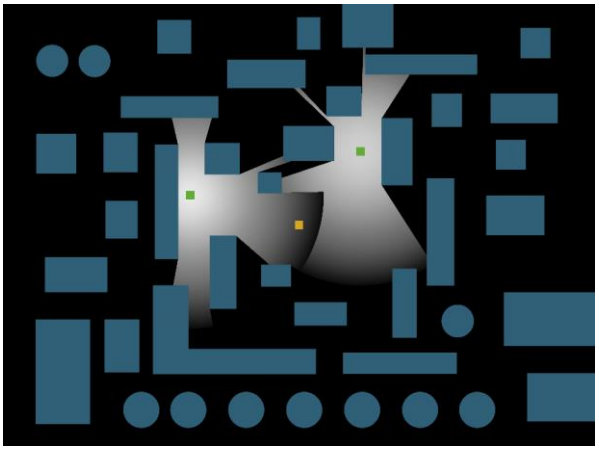


Рис. 5. Расчетная конфигурация поля обнаружения

Для простоты изложения в дальнейшем принимается, что степень идентификации факта проникновения нарушителя абсолютна, то есть в каждой точке внутри границы поля обнаружения вероятность выявления нарушителя равна единице.

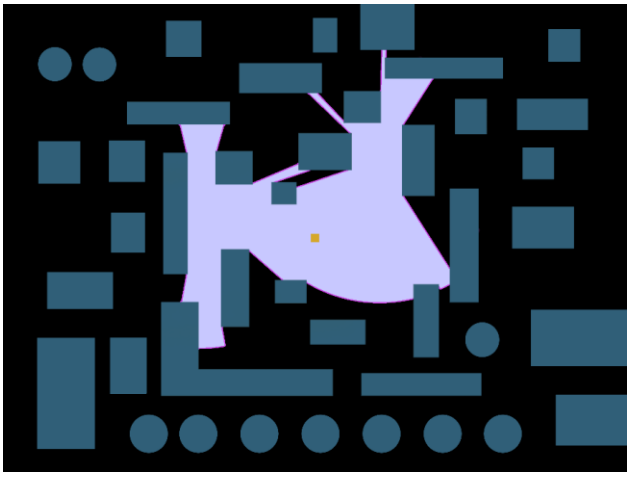


Рис. 6. Условная конфигурация поля выявления Z_{detect}

Определение исходной позиции нарушителя. При расчетах исходной позицией нарушителя может стать любая достижимая им точка на границе поля обнаружения, то есть элементы границы этого поля, подход к которым не блокируется препятствиями. Они легко определяются на основании данных о модели местности и поля обнаружения. Поле точек, отображающих возможные исходные позиции нарушителя, тонированное красным цветом, приведено на рис. 7. Обозначим совокупность этих точек через Z_{start}.

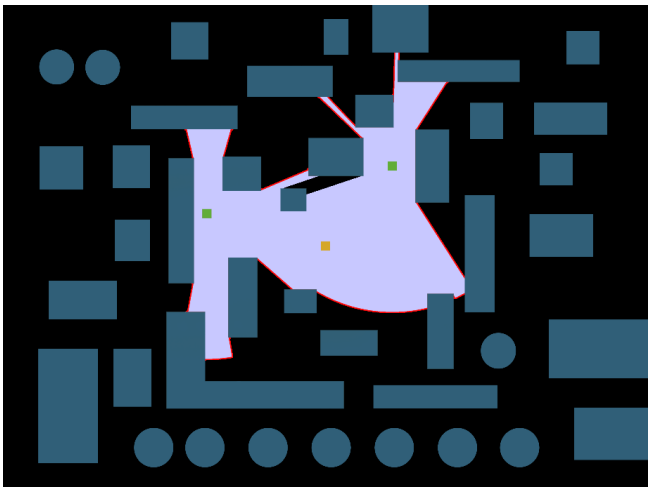


Рис. 7. Поле исходных позиций нарушителя Z_{start}

Расчет зоны скрытного проникновения. Введем понятие зоны скрытного проникновения – совокупность точек пространства внутри зоны досягаемости цели, достижение которых нарушителем осуществляется с

нулевой вероятностью обнаружения. Обозначим эту зоны через Z_s. Очевидно, что математически зона скрытного проникновения определяется как пересечение поля исходных позиций нарушителя по границе обнаружения и зоны досягаемости цели.

$$Z_s = Z_{start} \cap Z_{goal}. \quad (1)$$

Наложение этих зон можно видеть на рис. 8, где желтым цветом выделено поле досягаемости цели. Наличие и протяженность таких зон демонстрируют степень «открытости» объекта защиты. В принятом условном примере ввиду небольшого числа средств обнаружения выход нарушителя в зону досягаемости цели возможен с разных участков. Для примера стрелками показаны некоторые места пересечения соответствующих зон.

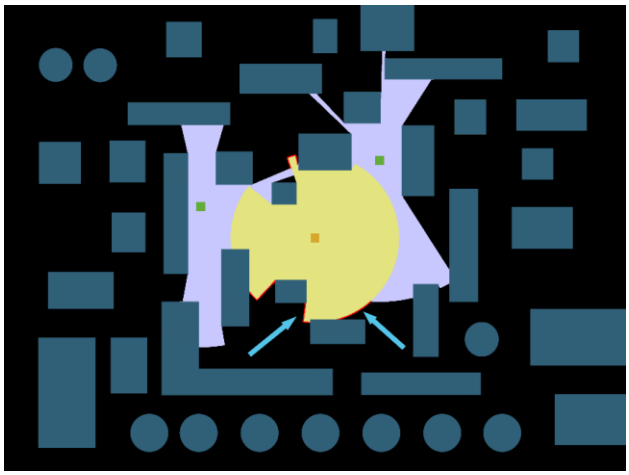


Рис. 8. Зоны скрытного проникновения Z_s на общей схеме зон

Определение зоны беспрепятственного движения. Помимо зон скрытного проникновения, наличие которых позволяет осуществить нападение на объект, минуя систему защиты, на уровень безопасности объекта влияет инерционность системы реагирования, то есть время принятия решения после получения информации о проникновении нарушителя. Наличие интервала времени между обнаружением нарушителя и выработкой решения на его нейтрализацию создаёт дополнительную возможность беспрепятственного движения к цели.

Учет инерционности системы реагирования может быть отражён путём введения ещё одной интегральной характеристики – зоны беспрепятственного движения, которая отображает совокупность точек пространства, достигаемых нарушителем за время, необходимое системе реагирования на принятие решения о его нейтрализации. При расчете этой зоны используются данные о скоростных характеристиках и исходной позиции нарушителя, а также о параметрах системы управления. В рассматриваемом примере предполагается, что нейтрализация нарушителя осуществляется в момент принятия этого

решения, что позволяет не рассматривать функционирование элементов собственно системы реагирования.

Результат расчета зоны беспрепятственного движения Z_{freeD} приведён на рис. 9. Указанная зона выделена розовым цветом.

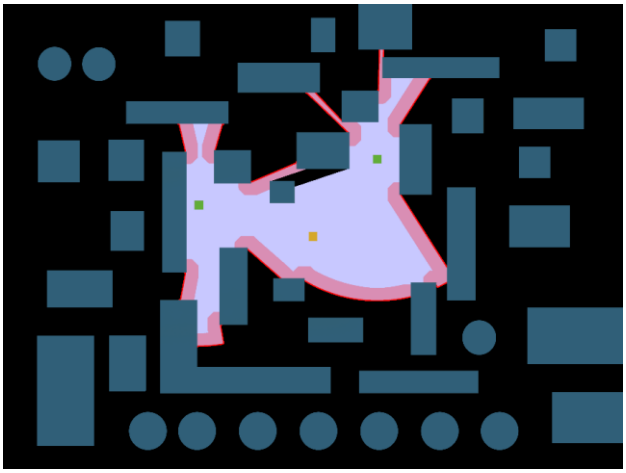


Рис. 9. Зона беспрепятственного движения Z_{freeD}

При расчётах зона беспрепятственного движения формируется как множество точек, длина кратчайшего пути от которых до точек ближайшей возможной исходной позиции нарушителя не превышает заданную величину. Последняя, в свою очередь, определяется как произведение скорости перемещения нарушителя на время выработки решения о его нейтрализации.

Расчет зоны неконтролируемого воздействия на целевой объект Под зоной неконтролируемого воздействия будем понимать часть зоны воздействия на целевой объект, которую способен достичь нарушитель до момента его нейтрализации.

Зона неконтролируемого воздействия рассчитывается как пересечение зоны воздействия на целевой объект с зоной беспрепятственного движения. Если обозначить эту зону через Z_{danger} , то её значение получим в виде:

$$Z_{danger} = Z_{goal} \cap Z_{freeD}. \quad (2)$$

Пример определения зоны неконтролируемого воздействия приведен на рис. 10, где эти зоны выделены светло-коричневым тоном на желтоватом поле.

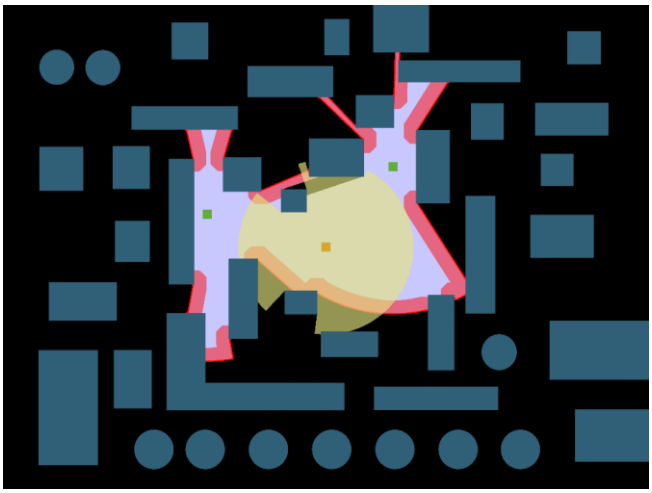


Рис. 10. Зона неконтролируемого воздействия на объект

Расчёт интегральных параметров. Полученные выше результаты пространственных расчетов могут служить основой для определения интегральных характеристик защищенности объекта, а именно:

- защищенности от скрытого проникновения,
- защищенности от открытого воздействия,
- интегрального показателя защищенности.

Соответствующие показатели можно рассчитать следующим образом.

Защищенность от скрытого проникновения. Для целей оценки системы обеспечения физической безопасности объекта показатель эффективности системы защиты от воздействия при скрытом проникновении может быть определен через вероятность скрытого воздействия, связанного со степенью информированности нарушителя, по следующей формуле (3):

$$P_h = \frac{Z_s}{Z_s + (1 - P_{info}) * (Z_{start} - Z_s)}, \quad (3)$$

в которой:

P_h – вероятность скрытого воздействия,

Z_s – длина участков зоны скрытого проникновения,

P_{info} – параметр информированности нарушителя об объекте,

Z_{start} – общая длина участков зоны исходной позиции.

Параметр информированности нарушителя задается в диапазоне [0,1], где «0» означает отсутствие информации о зонах обнаружения и досягаемости цели, «1» – полную информированность.

Уровень защищенности от скрытого проникновения тогда можно определить по формуле (4):

$$P_{sh} = 1 - P_h. \quad (4)$$

Защищенность от открытого проникновения. Аналогичным образом можно ввести показатель оценки эффективности системы защиты объекта от открытого воздействия, который может быть рассчитан в виде (5):

$$P_w = \frac{Z_{danger}}{Z_{danger} + (1 - P_{info}) * (Z_{freeD} - Z_{danger})}, \quad (5)$$

где:

P_w – вероятность открытого воздействия,

Z_{danger} – зона неконтролируемого воздействия,

Z_{freeD} – зона беспрепятственного движения,

P_{info} – информированность нарушителя о ситуации.

Уровень защищенности от открытого проникновения определяется по следующей формуле (6):

$$P_{sw} = 1 - P_w. \quad (6)$$

Сводный показатель защищённости объекта. Тогда сводный (интегральный) показатель защищенности объекта может быть вычислен через произведение вышеприведенных значений показателей каждого вида защищенности (7):

$$D = P_{sw} * P_{sh}. \quad (7)$$

Заключение

В данной статье предложен подход к оценке степени защищенности объекта путем расчетного определения ключевых параметров взаимодействия нарушителя с комплексной системой защиты объекта, а также вариантов их расположения на местности, которые позволяют получить интегральную оценку степени защищённости объекта. Ключевой особенностью приведенного здесь методического подхода является унарность (в противовес векторной) оценки показателя защищенности, что позволяет использовать этот подход для создания инструментов автоматической оптимизации размещения на местности средств обнаружения несанкционированного проникновения и средств противодействия несанкционированному воздействию (включая ударные средства поражения) с целью обеспечения максимальной защищенности целевого объекта.

Библиографический список

1. Методические рекомендации по разработке планов повышения защищенности критически важных объектов, территорий субъектов Российской Федерации и муниципальных образований. – М.: МЧС России, ФГБУ ВНИИ ГОЧС (ФЦ), 2011. - 37 с.

2. Трофименко Ю.В., Григорьева Т.Ю., Евгеньев Г.И., Иванов С.Б.. Обеспечение защищенности автомобильных мостов от актов незаконного вмешательства: учеб. пособие / под ред. Ю.В. Трофименко. – М.: МАДИ, 2014 – 172 с. ISBN 978-5-7962-0150-3.

3. Панин О.А. Как измерить эффективность? Логико-вероятностное моделирование в задачах оценки систем физической защиты / Безопасность – Достоверность – Информация. 2008. №2(77). с. 20-24.

4. Махутов Н.А., Балановский В.Л., Габур С.П.. Постановка проблемы по совершенствованию антитеррористической защищённости государственных важных объектов / Труды Международной научной конференции SCVRT2018, Институт физико-технической информатики, 2018, стр.1-13.

5. Балута В.И., Осипов В.П., Яковенко О.Ю. Среда моделирования, прогнозирования и экспертиз как интеллектуальное ядро поддержки управления сложными системами // Препринты ИПМ им. М.В.Келдыша. 2015, №82, 16 с. URL: http://library.keldysh.ru/preprint.asp?id=2015-82.

6. Осипов В.П., Четверушкин Б.Н., Нечаев Ю.И., Балута В.И. Онтологический синтез управленческих решений в условиях антагонистических конфликтов // Препринты ИПМ им. М.В.Келдыша. 2018. № 179. 28 с. doi:10.20948/prepr-2018-179; URL: http://library.keldysh.ru/preprint.asp?id=2018-179.

7. Осипов В.П., Четверушкин Б.Н., Балута В.И., Нечаев Ю.И. Формальный аппарат моделирования и интерпретации антагонистических конфликтов на базе электронного полигона // Препринты ИПМ им. М.В.Келдыша. 2018. № 181. 28 с. doi:10.20948/prepr-2018-181.

Оглавление

Введение 3
Описание алгоритма решения 5
Применение методики определения интегральных показателей 8
Заключение 16
Библиографический список 16