Модели противодействия терроризму: классификация

В. В. Шумов

Аннотация. В статье приведен краткий обзор современных работ по моделированию системы противодействия терроризму или элементов указанной системы. Также представлен вариант возможной классификации моделей терроризма и моделей системы противодействия терроризму.

Ключевые слова: *терроризм, система противодействия терроризму, математические модели, классификация моделей.*

Введение

Под терроризмом понимается «незаконное использование или угроза использования силы или насилия против отдельных лиц или имущества с целью принуждения или запугивания правительства или общества, часто для достижения политических, религиозных или идеологических целей» [1].

Терроризм является дешевым, неопасным, высокоэффективным средством и позволяет слабому бросать вызов сильному. Отдельные лица или группы лиц используют терроризм, чтобы достичь цели сверх их врожденных способностей. Терроризм дает слабому государству недорогую форму борьбы, в то время как более сильные государства используют терроризм, чтобы осуществлять тайные операции. К террористическим акциям относятся взрывы, поджоги, похищение транспортных средств, угон и похищение самолетов и морских судов, засады, похищение людей, взятие заложников, поддержка международных наркодельцов, грабеж и вымогательство, психологический террор, нападение с использованием ядерного, биологического и химического оружия, убийства [1].

В соответствии с федеральным законом [2], противодействие терроризму включает следующие направления деятельности:

- предупреждение терроризма, в т. ч. выявление и устранение причин и условий, способствующих совершению террористических актов (*профилактика терроризма*);
- выявление, предупреждение, пресечение, раскрытие и расследование террористического акта (*борьба с терроризмом*);
- минимизация и (или) *ликвидация последствий* проявлений терроризма.

Концепция противодействия терроризму в Российской Федерации [3] определяет основную форму пресечения террористического акта — *контртеррористическую операцию*, которая предусматривает реализацию комплекса специальных, оперативно-боевых, войсковых и иных мероприятий с применением боевой техники, оружия и специальных средств по пресечению террористического акта, обезвреживанию террористов, обеспечению безопасности граждан, организаций и учреждений, а также по минимизации и (или) ликвидации последствий проявлений терроризма. К условиям антитеррористической деятельности относятся: нормативно-правовые, информационно-аналитические, научно-методические, материально-технические, финансовые и кадровые условия.

В соответствии с теорией оперативно-розыскной деятельности [4], для борьбы с терроризмом могут использоваться следующие формы и виды оперативно-розыскных мероприятий: личный сыск[1], оперативный эксперимент[2], оперативная комбинация[3], оперативный поиск[4], оперативная разработка[5] и др.

[1] Личный сыск — обнаружение, выявление, поиск, розыск, осуществляемое лично субъектом этих действий.

[2] Оперативный эксперимент — воспроизведение действий, обстановки или иных обстоятельств противоправного события и совершение необходимых опытных.

[3] Оперативная комбинация — комплекс действий, объединенных единым замыслом, легендой и направленных на решение конкретной задачи обнаружения, предотвращения или раскрытия преступления.

[4] Оперативный поиск предполагает получение и проверку первичной информации о лицах и фактах, представляющих оперативный интерес, вне связи с конкретным лицом или фактом с последующим выделением последних из общей массы.

[5] Оперативная разработка — форма оперативной деятельности, которая проводится в отношении конкретных лиц (групп), подозреваемых в причастности или причастных к подготовке или совершению преступлений, и целью которой является наиболее полное вскрытие преступной деятельности разрабатываемых и подготовка мер ее пресечения.

В США используется трехуровневая концепция борьбы с терроризмом (разработка процедур государственной политики и управления; координация и контроль; оперативные процедуры для *сдерживания*, *предотвращения*, *противодействия* и *прогнозирования* террористической деятельности). Руководством [1] даются определения основных понятий:

- *антитерроризм* (antiterrorism) — защитные (пассивные) меры, используемые для снижения уязвимости как отдельных лиц, так и собственности акциям терроризма;
- *контртерроризм* (counterterrorism) — наступательные (активные) меры, предпринимаемые для выявления, предупреждения и пресечения акций терроризма;
- *борьба с терроризмом* (combating terrorism) — действия анти- и контртеррористического характера;
- *сдерживание* (deterrence) — сдерживание от совершения каких-либо действий при помощи внушения страха последствий этих действий. Сдерживание — это состояние ума, вызванное существованием реальной угрозы ответных действий;
- *предотвращение* (prevention) — меры безопасности, предпринятые общественностью или частным сектором, с целью отбить у террористов намерение совершить теракт;
- *реакция* (reaction) — проведение контртеррористических операций в ответ на определенные акции терроризма;
- *анализ угрозы* (threat analysis) — анализ уязвимости объекта с точки зрения совершения на нем теракта с целью вскрытия и устранения слабых сторон в системе безопасности объекта.

После теракта 11 сентября 2001 г. в США было создано Министерство внутренней безопасности (DHS) с целью достижения оптимального взаимодействия всех ведомств для предотвращения террористических актов и борьбы с последствиями стихийных бедствий. Одна из задач ведомства — организация научных исследований в области безопасности и противодействия терроризму.

1. Классификация и характеристика моделей противодействия терроризму

1.1. Классификация и характеристика моделей по уровню абстракции/конкретности [5, с. 26]: концептуальные модели, модели анализа и синтеза, реализация

1.1.1. ***Концептуальные модели*** — разрабатываются специалистами предметной области, политологами, психологами, социологами и др. В качестве примера можно привести работу «Social Science for Counterterrorosm. Putting the Pieces Together» [6]. В названной работе приведены эмпирические данные по моделям принятия решений участниками террористических организаций на различных уровнях.

Модель принятия решений на стратегическом уровне. На стратегическом уровне конечной целью террористов является максимизация наносимого ущерба своим врагам. Было проанализировано влияние терроризма на потребление, инвестиции, экспорт и ВВП на душу населения в Израиле. Исследователи пришли к выводу, что если бы Израиль не пострадал от терроризма в 2000–2003 гг., то ВВП на душу населения был бы на 10 % выше, чем его реальный уровень. Помимо прямого экономического ущерба, террористические атаки вызывают выгодные организаторам психологические реакции населения.

Модель принятия решений на тактическом и оперативном уровнях. Анализируя действия руководителей террористических групп, исследователи пришли к выводу, что они действуют рационально, т. е. выбирают объект атаки, исходя из целевой привлекательности, осуществимости, эффективности и стоимости. Статистические данные показали, что руководители террористических групп посылали на более важные цели террористов-смертников с высшим образованием и/или зрелого возраста.

Модель принятия решений на уровне отдельного террориста. Террористы являются, как правило, выходцами из среднего класса, преимущественно мужчинами в возрасте 17–30 лет. Причем отдельные террористы в среднем богаче и образованнее, чем социальная среда, из которой они рекрутируются. Их мотивы поведения — альтруизм, чувство ответственности перед будущими поколениями, религиозная мотивировка, политический активизм.

Показано, что на всех уровнях террористы действуют рационально (ограниченно рационально), что создает предпосылки для применения математического аппарата в интересах повышения эффективности контртеррористических мер.

Члены террористических групп подразделяются на признанных лидеров, действующий кадровый состав, активных сторонников и пассивных сторонников. Террористами используются следующие источники сбора разведывательной информации: агентурная разведка; радиотехническая разведка; фоторазведка; анализ типовых операций [1].

А. Уилнер в статье «Понятие сдерживания времен холодной войны работает против терроризма» отмечает: если мы думаем о терроризме как о группе людей, действующих согласованными усилиями для достижения единой цели, тогда мы можем подумать и о том, чтобы выбрать группу целей внутри этой организации, которыми мы можем манипулировать с точки зрения логики сдерживания [7]. По мнению А. Уилнера включение теории сдерживания в войну с терроризмом путем ослабления соотношения за-

трат к выгоде в вопросе осуществления атаки, позволит заблаговременно манипулировать поведением террористических групп.

1.1.2. ***Модели анализа и синтеза***. Как правило, это преимущественно математические или физические модели. В США разработка соответствующих исследований координируется и финансируется Министерством внутренней безопасности (DHS). Обзор важных с точки зрения DHS моделей анализа и синтеза дан в работе «A Survey of Operations Research Models and Applications in Homeland Security» [8]. Модели классифицированы по двум основаниям:

- циклы деятельности (*planning* — планирование, *prevention* — предотвращение, *response* — реагирование, *recovery* — восстановление);
- категории:
  - *countermeasures* — контрмер: Biological, Chemical, Radiological and nuclear, high explosives — физические модели;
  - *component support* — эффективность направлений: border security, airline security, port and rail, truck; critical infrastructure protection — защита критически важной инфраструктуры;
  - *cyber security* — компьютерная и интернет-безопасность;
  - *emergency preparedness and response* — готовность к чрезвычайным ситуациям и реагирование).

В обзоре [8] охарактеризованы и классифицированы более 60 работ. В частности, T. J. Sullivan и W. L. Perry [9] разработали основу для развития классификации террористических групп химического, биологического, радиологического и ядерного оружия с использованием эвристического метода распознавания образов, метода деревьев классификации и дискриминантного анализа. Применительно к системам безопасности на транспорте ряд работ посвящен анализу устройств с целью повышения вероятности обнаружения и снижения интенсивности ложных тревог. E. Pate-Cornell [10] с использованием байесовского анализа разработал метод ранжирования угроз и назначения приоритетов мерам безопасности и объектам.

1.1.3. ***Технологии и документы, созданные на основе моделей*** **(*реализация*)**. Руководство силами морской пехоты флота «Борьба с терроризмом» [1] требует изменять шаблоны действий антитеррористических и военных подразделений с целью дезориентации террористов и повышения их риска. Рекомендуется повышать вероятность случайных действий путем изменения районов, маршрутов и графиков патрулирования; выборочной проверки пассажиров и транспортных средств, организуемой с использованием случайного чередования признаков (цифры номера машины, количество пассажиров и т. д.).

Некоторые модели находят практическое применение и встраиваются в программное обеспечение. Одно из важнейших требований к моделям — учет большого количества факторов. По оценке Д. Ю. Каталевского модели, отвечающие запросам руководителей, обычно включают от 30 до 3000 переменных. Нижний предел близок к тому минимуму, который отражает основные типы поведения системы, интересующие тех, кто принимает решения. Верхний предел ограничивается нашими возможностями восприятия системы и всех ее взаимосвязей [11].

В этой связи на практике обычно используются комплексные модели с параметрами, измеренными в различных шкалах. Рассмотрим теоретико-игровую модель для обеспечения безопасности в международном аэропорту г. Лос-Анджелес [12], на основе которой разработана и введена в эксплуатацию автоматизированная система «Помощник для рандомизированного контроля маршрутов» (ARMOR — Assistant for Randomized Monitoring over Routes). Безопасность в основных местах социально-экономической и политической активности является ключевой во всем мире, особенно с учетом угрозы терроризма. Вместе с тем ограниченные ресурсы не позволяют силам безопасности круглосуточно контролировать все объекты и маршруты. Террористы способны вести наблюдение и выбирать не охраняемые маршруты и объекты для атаки, если силы безопасности не используют рандомизированную тактику патрулирования и мониторинга.

Авторы формулируют основные требования к «Помощнику».

1. «Помощник» должен учитывать веса охраняемых объектов. Если нападение на первый объект приведет к экономическому ущербу, а на второй — к человеческим жертвам, то больший вес должен быть присвоен второму объекту. Веса оцениваются экспертами и выражаются в порядковой шкале.
2. «Помощник» должен учитывать всю имеющуюся у службы безопасности информацию о противнике.
3. «Помощник» не должен предлагать жесткий график несения службы. У пользователей должна быть возможность вносить корректировки, учитывая тем самым дополнительные сведения.

«Помощник» эксплуатируется с августа 2007 г. M. Taylor и др. [13] описали тесты для проверки «Помощника»:

- анализ теории игр (тип теста — Mathematic): при известных матрицах выигрышей вычисляется выигрыш агента и вероятность отказа от попытки правонарушения;
- распределение ресурсов (тип теста — Mathematic): теория игр помогает найти ожидаемый выигрыш агента при различных стратегиях Лидера;

- стоимость защиты (тип теста — Mathematic): теория игр помогает найти ожидаемые выигрыши сторон при изменении технологии охраны (ввод в эксплуатацию новых технических средств охраны или нового процесса проверки багажа);
- имитация атаки (тип теста — Simulation): использование дополнительных имитационных моделей;
- пуски учебных нарушителей (тип теста — Human): исследования психологии человека в условиях физиологических стрессов помогают имитировать поведение агентов. недостаток таких тестов — учебные нарушители не принадлежат той же среде, что и реальные агенты;
- экспертные оценки (тип теста — Qualitative): специалисты служб безопасности способны оценить многие факторы для их последующего учета в модели в качестве параметров.

С 2009 г. «Помощник» стал использоваться для планирования службы воздушных патрульных (Marshals Service) с задачей оптимального распределения 3 000–4 000 патрульных (аэромаршалов) по 29 000 ежедневных самолето-вылетов.

Проектные решения, связанные с масштабированием системы на территорию страны (400 аэропортов), описаны в работе [14]. В ходе реализации программы внедрения системы были решены проблемы, связанные с наличием сотен разнородных пунктов охраны и большим разнообразием угроз, и применен частично централизованный подход к обучению персонала и развитию системы.

1.2. Матрицы моделей противодействия терроризму

Сложность реальных ситуаций, связанных с обеспечением безопасности, требуют универсальности применяемых математических моделей. Эти требования неизбежно приходят в противоречие с общностью и обоснованностью результатов моделирования, поэтому при решении реальных задач применяется комплекс моделей в виде иерархии (обычно более низким уровням иерархии соответствует более высокая степень детализации описания моделируемых систем) или горизонтальной цепочки, в каждом элементе которой степень детализации примерно одинакова [15].

В табл. 1 представлены уровни моделирования (иерархии моделей) противодействия терроризму.

Циклы, связанные с противодействием терроризму:

- цикл борьбы с терроризмом: Planning — планирование, Prevention — предотвращение, Response — реагирование, Recovery — восстановление [8];
- цикл специальной операции по задержанию преступников: Сбор информации — Режимные действия — Нейтрализация [4];
- цикл преступного поведения: Формирование мотивации — Принятие решения, планирование — Исполнение решения — Посткриминальное поведение [16],

имеют качественно разные этапы, которые не всегда удается объединить в рамках одной модели. Поэтому используются цепочки моделей, где отдельная модель соответствует определенному этапу цикла деятельности.

Объединение двух подходов, иерархического и горизонтального (на основе циклов деятельности и управления), позволяет говорить о матричных моделях.

На каждом из уровней иерархии модели дополнительно классифицируются по следующим основаниям.

1.2.1. По *видам терактов:*

- модели противодействия актам с применением обычных средств поражения и взрывчатых веществ;
- модели противодействия актам с применением ядерных, химических и биологических элементов;
- модели противодействия кибернетическому терроризму;
- модели противодействия информационному терроризму;
- модели противодействия экономическому терроризму.

1.2.2. По *среде:*

- модели противодействия на суше;
- модели противодействия в воздушном пространстве;
- модели противодействия в морском пространстве;
- модели противодействия в киберпространстве;
- модели противодействия в информационном пространстве.

1.2.3. По *видам террористических организаций:*

- модели противодействия государственным террористическим организациям;
- модели противодействия негосударственным террористическим организациям;
- модели противодействия одиночным террористам.

1.2.4. По *мотивации:*

- модели противодействия терроризму с политико-идеологической (религиозной) мотивацией;
- модели противодействия терроризму с криминальной мотивацией.

1.2.5. По *методу моделирования:*

- теоретико-игровые модели;
- оптимизационные модели;
- имитационные модели.

Таблица 1

Уровни моделирования противодействия терроризму

Моделируемые явления (процессы)	Задачи моделирования
1. *Уровень среды*	
Использование геоинформационных, метеорологических, гидрологических и других данных, характеризующих внешнюю среду и объекты охраны и определяющих параметры движения и возможности атакующих (террористов) и защитников	Построение маршрутов и сетей движения атакующих и защитников, определение непроходимых (неиспользуемых) участков и районов, расчет временны́х параметров движения для различных условий, выбор мест возможной установки средств защиты и др.
2. *Уровень террористического средства*	
Поражающие факторы террористического средства (обычное оружие, ядерное, химическое, биологическое и др.)	Построение зон поражения с учетом среды для различных объектов и средств доставки
3. *Информационно-технический уровень*	
Возможности по обмену информацией между атакующими (и их пособниками) и между защитниками	Построение и оптимизация сетей информационного обмена, разведка и защита сетей
4. *Системно- и социо-технический уровень*	
Объединение разнородных средств в единую систему атакующих (защитников). Анализ системы «человек-машина» с точки зрения выполнения ею тактических задач	Расчет надежности системы, построение и оптимизация единой системы. Расчет готовности системы, обоснование системы эксплуатации и сопровождения; обоснование требований к рабочим местам
5. *Операционный уровень*	
Реализация действий: порядок и правила несения службы (совершения теракта), маскировки, преследования, нейтрализации и т. д.	Оптимизация действий одиночных и групповых средств атакующих (защитников)
6. *Тактический уровень*	
Действия террористических групп, способных нанести ущерб малой и средней степени тяжести. Действия защитников на уровне подразделения (района)	Моделирование и оптимизация действий подразделения (групп, банд)
7. *Оперативный уровень*	
Действия террористических групп, способных нанести ущерб высокой степени тяжести. Действия защитников на уровне региона	Моделирование и оптимизация противодействия терроризму на уровне региона
8. *Стратегический уровень*	
Действия террористических групп и защитников на уровне государства (нескольких государств). Проектирование противодействия терроризму	Оценка систем, факторов и процессов, способных порождать террористические угрозы. Анализ рисков и построение сценариев
9. *Уровень целеполагания*	
Проектирование концепции противодействия терроризму. Выбор целей, проектирование механизмов воздействий и механизмов функционирования	Моделирование развития систем противодействия терроризму

Теоретико-игровые модели борьбы с терроризмом относятся к классу Security Game [17; 18; 19]. Их можно найти в экономических, политических, компьютерных и иных исследованиях. Одно из решений — моделирование в области безопасности на основе байесовских игр [20], в которых полагается известным распределение противника по типам. В некоторых работах [21] для поиска оптимальных стратегий сторон используется игра полковника Блотто. К сожалению, в них не учитывается очевидный факт, что противник способен вести наблюдение за системой охраны (защитником) и использовать эту информацию.

Б. Голэни и др. в работе [22] обсуждают концепции и механизмы выделения государственных ресурсов на внутреннюю безопасность США, основываясь на понятиях вероятностный риск (probabilistic risk) и стратегический риск (strategic risk).

Д. С. Файнштейн и Э. Х. Каплан в статье «Analysis of a Strategic Terror Organization» [23] моделируют выбор террористическими организациями масштаба и горизонта планирования террористических атак

и влияние последствий этого выбора на развитие организаций.

Д. Калкинс и др. [24] рассматривают модель оптимального управления борьбы с терроризмом, учитывающую уровень общественных симпатий к антитеррористическим силам.

2. Примеры работ по моделированию борьбы с терроризмом

2.1. Характеристика теоретико-игровой модели для обеспечения безопасности аэропорта

В модели служба безопасности именуется Лидером, а потенциальные террористы различных типов — агентами. Задача — найти оптимальную смешанную стратегию Лидера в предположении, что агенты, возможно, знают эти стратегии и учитывают их при выборе своих действий.

Формальная постановка задачи:

$$\max_{x,q,a} \sum_{i\in X}\sum_{l\in L}\sum_{j\in Q} p^l R^l_{ij} x_i q^l_j \,, \qquad (1)$$

$$\sum_{i\in X} x_i = 1\,,\ \sum_{j\in Q} q^l_j = 1\,,\ 0 \le \left(a^l - \sum_{i\in X} C^l_{ij} x_i \right) \le \left(1 - q^l_j\right) M \,,$$

$$x_i \in [0...1]\,,\ q^l_j \in \{0,1\}\,,\ a \in \Re \,,$$

где: x — вектор-стратегия Лидера (x_i — доля времени, в течение которого используется i-я стратегия);

q^l — вектор-стратегия агента типа l;

R^l и C^l — матрицы выигрышей Лидера и агента типа l;

M — большое положительное число;

p^l — априорная вероятность агента типа l.

Первое и четвертое ограничения определяют множество возможных действий Лидера как распределение вероятностей на множестве X. Второе и пятое ограничения определяют множество возможных действий агента типа l. Каждый агент l имеет строго одну единичную стратегию. Третье ограничение работает следующим образом:

- левая часть неравенства означает, что a^l есть верхняя граница выигрыша агента l;
- для действия $q^l_j = 1$ правая часть неравенства означает, что это действие должно быть оптимальным для агента l.

Задача лидера — проверять объекты аэропорта и контролировать транспортные потоки на пунктах пропуска (имеется n дорог к аэропорту). Применительно к пунктам пропуска опишем множество X. Если Лидер в одно время может выставить только один пункт пропуска, то $X = \{1, \ldots, n\}$; при двух пунктах пропуска $X = \{(1, 2), (1, 3) \ldots (n-1, n)\}$ и т. д. Каждый агент $l \in L = \{1,...,m\}$ может принять решение использовать для атаки одну из дорог или не атаковать совсем. Тогда его множество всех действий $Q = \{1, \ldots, n, none\}$.

Если Лидер выбрал дорогу i для проверки, а агент l — дорогу j, то Лидер получает вознаграждение R^l_{ij}, а агент — C^l_{ij}. Если Лидер задерживает агента, то его выигрыш положителен, а выигрыш агента отрицателен. Интенсивность потока машин на дорогах и ценность этих дорог для агентов учитываются посредством назначений значений выигрышей.

Заменой $z^l_{ij} = x_i q^l_j$ задача (1) сводится к задачам целочисленного линейного программирования.

2.2. Модели распределения ресурсов для обеспечения безопасности объектов

Боуз Голэни и др. предложили концепции и механизмы выделения государственных ресурсов по объектам в целях обеспечения внутренней безопасности государства [22].

2.2.1. ***Распределение ресурсов в условиях вероятностного риска***. Введем следующие обозначения:

- π_i — вероятность того, что i-й объект ($i = 1, \ldots, n$) подвергнется удару стихии;
- $0 \le p_i < 1$ — (условная) вероятность того, что объект i будет разрушен в случае атаки на него при отсутствии мер по защите;
- $C_i > 0$ — нанесенный ущерб объекту i;
- $\alpha_i > 0$ — коэффициент эффективности использования ресурсов на объекте i.

В случае отсутствия каких-либо действий по защите объекта i *ожидаемый ущерб* равен $\pi_i p_i C_i$. Ожидаемый ущерб может быть уменьшен за счет выделения ресурсов.

Пусть B есть объем ресурса, который может выделить государство (ведомство) на защиту объектов. Обозначим $x_1, x_2, \ldots, x_n$ — ресурсы, выделенные на защиту объектов $i = 1, 2, \ldots, n$.

Цель государства (ведомства) — свести к минимуму суммарный ущерб. Получим следующую оптимизационную задачу:

$$\psi = \sum_{i=1}^{n} \pi_i C_i (p_i - \alpha_i x_i) \to \min_x \,, \qquad (2)$$

$$\sum_{i=1}^{n} x_i \le B \,, \qquad (3)$$

$$0 \le x_i \le p_i / \alpha_i \,,\ i = 1, \ldots, n. \qquad (4)$$

Перенумеруем объекты так, чтобы выполнялось неравенство:

$$\pi_{i_1} C_{i_1} \alpha_{i_1} \ge \ldots \ge \pi_{i_n} C_{i_n} \alpha_{i_n} \,. \qquad (5)$$

Тогда оптимальное распределение ресурсов заключается в следующем. На первый объект необходимо выделить

$$x_{i_1}^* = \min\left(p_{i_1}/\alpha_{i_1}, B\right),$$

на второй

$$x_{i_2}^* = \min\left(p_{i_2}/\alpha_{i_2}, B - x_{i_1}^*\right)$$

и т. д. до исчерпания ресурса или обеспечения защиты всех объектов.

2.2.2. ***Распределение ресурсов в условиях стратегического риска.*** Предположим, что противник (террористы) имеет полную информацию о состоянии объектов и стремится нанести государству максимальный ущерб.

В условиях стратегического риска задача поиска оптимального распределения ресурсов имеет вид:

$$\theta = \max_{i=1,\ldots,n} C_i(p_i - \alpha_i x_i) \to \min_x, \tag{6}$$

$$\sum_{i=1}^{n} x_i \le B, \tag{7}$$

$$0 \le x_i \le p_i/\alpha_i, \; i = 1, \ldots, n. \tag{8}$$

Обозначим θ^* — значение целевой функции при оптимальном распределении ресурсов. Ожидаемый ущерб при оптимальном распределении ресурса соответствует условию

$$C_i(p_i - \alpha_i x_i^*) = \begin{cases} \theta^*, & C_i p_i \ge \theta^*, \\ C_i p_i, & C_i p_i < \theta^*, \end{cases} \tag{9}$$

или в эквивалентной записи:

$$x_i^* = \begin{cases} \left(C_i p_i - \theta^*\right)/C_i\alpha_i, & C_i p_i \ge \theta^*, \\ 0, & C_i p_i < \theta^*. \end{cases} \tag{10}$$

Заметим, что из (9) следует

$$C_i(p_i - \alpha_i x_i^*) \le \theta^*, \; i = 1, \ldots, n. \tag{11}$$

Перенумеруем объекты так, чтобы выполнялось неравенство

$$C_{i_1} p_{i_1} \ge \ldots \ge C_{i_n} p_{i_n}. \tag{12}$$

Обратим внимание, что данное условие отличается от условия (5). Алгоритм выделения ресурса в условиях стратегического риска следующий. На самый важный i_1-й объект выделяем ресурс до тех пор, пока он не исчерпается или ожидаемые потери на нем станут равными потерям на объекте i_2:

$$x_{i_1,1}^* = \min\left(\left(C_{i_1} p_{i_1} - C_{i_2} p_{i_2}\right)/C_{i_1} p_{i_1}, B\right).$$

На втором этапе распределяем ресурсы таким образом, чтобы сумма ожидаемых потерь на объектах i_1 и i_2 стала равной потерям на объекте i_3 и т. д.

Введя фиктивный объект $n + 1$, для которого $p_{n+1} = 0$, $C_{n+1} = \alpha_{n+1} = 1$, получим выражение для оптимального значения целевой функции:

$$\theta^* = \begin{cases} C_{i_{t^*}} p_{i_{t^*}} + \dfrac{B - \sum\limits_{s=1}^{t^*}\left(C_{i_s} p_{i_s} - C_{i_{t^*}} p_{i_{t^*}}\right)/C_{i_s}\alpha_{i_s}}{\sum\limits_{s=1}^{t^*} C_{i_s}\alpha_{i_s}}, & t^* \le n, \\ 0, \quad t^* = n+1, \end{cases} \tag{13}$$

$$t^* \equiv \max\left(t = 1, \ldots, n+1 : \sum_{s=1}^{t^*} \frac{C_{i_s} p_{i_s} - C_{i_t} p_{i_t}}{C_{i_s}\alpha_{i_s}} \le B\right). \tag{14}$$

Таким образом, оптимальное управленческое решение существенно зависит от вида риска.

2.3. Модель защиты транспортных сообщений

Д. Стренланд и Б. Филд [25] рассматривают модель распределения фиксированного бюджета для защиты путей, с использованием которых террористы совершают атаки и для смягчения ущерба от атак.

Пусть N есть число путей, используя которые, террористы совершают атаки. Полагается, что пути идентичны и террористам безразлично, какой из них выбрать. Вероятность p атаки посредством любого из путей не превышает некоторого порогового значения $p_c \le 1$. Для защиты от возможного нападения защищается $n \le N$ путей (выбираются в случайном порядке). Следовательно, вероятность успешной атаки равна $p\,(N - n)\,/\,n$.

В случае успеха атаки общество несет потери L. Усилия m государства по их смягчению уменьшают потенциальные потери. Полагается $L'(m) < 0$ и $L''(m) > 0$.

Пусть $\bar{L}$ есть критическое значение потерь от террористической атаки. Рассмотрим проблему максимизации диапазона вероятности атаки, внутри которого ожидаемые потери не превышают критических:

$$\max_{p \in [0, p_c]} L(m)p(N-n)/N \le \bar{L}, \; n \in [0, N], \; m \ge 0$$

или

$$p(n, m, \bar{L}, p_c) = \frac{\bar{L}N}{L(m)p(N-n)}, \; n \in [0, N], \; m \ge 0.$$

Обозначим через R денежные ресурсы, выделяемые на защиту от терроризма, w_n и w_m — расходы на один путь и единицу усилий по смягчению атаки со-

ответственно. Эффективное распределение ресурсов можно найти, решая следующую задачу:

$$\max_{n,m} p(n,m,\bar{L},p_c) = \frac{\bar{L}N}{L(m)p(N-n)}, \qquad (15)$$

$$R \geq w_n n + w_m m,$$

$$p(n,m,\bar{L},p_c) \leq p_c,$$

$$n \in [0,N],\ m \geq 0.$$

Задача (15) решается с использованием правила множителей Лагранжа.

2.4. Географическое профилирование[6]

Актуальной задачей является задача прогнозирования мест возможного базирования террористических групп.

В работе [26] описана модель, позволяющая предсказывать место жительства серийного преступника и прогнозировать место следующего преступления.

На практике для решения указанной задачи используются, как правило, следующие методы.

1. Метод окружности. Через две точки — координаты самых удаленных мест преступлений, проводится окружность. Центр окружности принимается за место жительства преступника.

2. Метод «центра масс». Вычисляется среднее арифметическое координат мест преступлений.

3. Метод с использованием формулы Rossmo.

Территория с использованием электронной карты покрывается сеткой с квадратными ячейками. Вероятность того, что преступник находится в ячейке (i — номер строки, j — номер столбца) может быть вычислена по формуле Rossmo [27]:

$$P_{i,j} = k\sum_{c=1}^{T}\left[\frac{\phi}{\left(|x_i - x_c| + |y_i - y_c|\right)^f} + \frac{(1-\phi)B^{g-f}}{\left(2B - |x_i - x_c| - |y_i - y_c|\right)^g}\right],$$

где: $f = g = 1{,}2$ — параметры;

k — параметр, обеспечивающий значение вероятности на отрезке [0, 1];

T — количество преступлений;

$0 \leq \phi \leq 1$ — весовой коэффициент;

B — радиус буферной зоны (буферная зона — это зона вблизи места жительства преступника, где он не совершает преступлений).

Формула Rossmo основана на двух предположениях:

- преступники не стремятся далеко ездить для совершения преступления;
- существует буферная зона вокруг места жительства преступника, где преступления не совершаются.

П. Шакариан и его коллеги в работе «Adversarial Geospatial Abduction Problems» [28] предложили теоретико-игровой подход к проблеме географического профилирования. Созданная на основе математической модели компьютерная программа SKARE прошла апробирование в Ираке для борьбы с повстанцами и террористами.

Тактика применения самодельных взрывных устройств (СВУ) террористами и повстанцами заключается в следующем [29]. Нападения с использованием СВУ осуществляются мелкими группами. В группе есть специалист по изготовлению СВУ, специалист по логистике и переносчик СВУ. Так же выделяется лицо, ответственное за установку и подрыв СВУ. Группы пользуются услугами информаторов и пособников из числа местного населения. Члены диверсионных групп не хранят СВУ дома. Для хранения используются склады (тайники, укрытия), к которым предъявляются определенные требования. Расстояние между складом и местом диверсии не может быть слишком малым, что чревато его раскрытием и уничтожением. С другой стороны, это расстояние не может быть слишком большим, поскольку велик риск быть обнаруженным на маршруте доставки. Обычно перевозка СВУ выполняется ночью, причем время доставки СВУ к месту диверсии не превышает одного-двух часов.

В программу SKARE введено ограничение — определенные нападения и тайники приписываются к одной диверсионной группе (или семейству групп). Для тестирования программы были взяты данные о диверсионных актах, совершенных в Багдаде (27 × 25 км) и его пригороде Садр-Сити (7 × 7 км) (табл. 2).

Точность определения координат тайника с СВУ по Багдаду составила 0,72 км. Низкая точность может быть объяснена значительной неоднородностью кварталов Багдада. Для более однородного по условиям совершения терактов пригорода точность составила 0,35 км [30].

Программа SKARE приспособлена для выявления тайников в городских кварталах, но мало пригодна для решения той же задачи в масштабе провинции Афганистана.

П. Шакариан внес доработки в теоретико-игровую модель, позволившую учитывать особенности рельефа двух провинций (площадь 580 на 430 км),

[6] Географическое профилирование — розыскная методология анализа мест совершения серии преступлений с целью выявления места проживания преступника. Включает качественные и количественные методы. Используется для поиска субъектов, совершивших серийные убийства, изнасилования, поджоги, взрывы бомб и т. д.

Таблица 2

Данные о диверсионных актах и их параметрах [30]

Область	Число диверсионных актов	Минимальное расстояние α, км	Максимальное расстояние β, км
Багдад	73	0,6	1,98
Садр-Сити	40	0	1,06

социально-культурные аспекты (разные племена, живущие в провинциях), возможности и режим полетов беспилотных летательных аппаратов и других средств войсковой разведки [31]. Для тестирования доработанной программы SKARE2 в нее были введены данные по 203 террористическим актам (103 случая использовались для определения границ интервалов $[\alpha, \beta]$ и 100 случаев для проверки точности прогнозирования мест СВУ). Программа SKARE2 позволяет определять местонахождение террористов и СВУ с точностью до 100 кв. км (в среднем это 4,6 села).

Заключение

Рассмотренные классификации и характеристики моделей противодействия терроризму позволяют сделать следующие выводы:

- практическую реализацию получили комплексные модели, сочетающие теоретико-игровой подход, имитационное моделирование и учет в расчетах экспертных оценок специалистов службы безопасности;
- применяемые на практике модели перекрывают с 1-го по 7-й уровень моделирования (табл. 1).

Многие рассмотренные модели имеют качественный характер, т. е. выполняют преимущественно дескриптивную функцию. Это объясняется главным образом следующими причинами:

- для моделей не выполнена оценка параметров;
- модели не носят комплексного характера, т. е. пропущены некоторые уровни моделирования;
- при планировании действий защитника на оперативном уровне делается попытка опуститься на тактический уровень (на тактическом уровне — на операционный уровень), поскольку это противоречит принципам управления [32].

Исходя из краткого обзора работ по предложенным классификациям, представляется актуальным и важным следующие направления исследований:

- перенос хорошо себя зарекомендовавших моделей в другие области (сферы) борьбы с терроризмом, например, применение моделей охраны аэропорта службой береговой охраны [32];
- разработка моделей стратегического уровня и уровня целеполагания.

Характерное время цикла проектирования и реализации концепции противодействия терроризму может составлять десятки лет, в связи с чем для прогноза развития обстановки целесообразно использовать, в частности, сценарный и фьючерсный[7] подходы. Пример их применения можно найти в работе [33].

Литература

1. FMFM 7–14 Combating Terrorism (USMC), 5 October 1990.
2. Федеральный закон от 06.03.2006 № 35-ФЗ (ред. от 08.11.2011) «О противодействии терроризму».
3. Концепция противодействия терроризму в Российской Федерации. Утверждена Президентом Российской Федерации Д. Медведевым 5 октября 2009 г. // «РГ» — Федеральный выпуск № 5022 20 октября 2009 г.
4. Теория оперативно-розыскной деятельности: учебник / Под ред. К. К. Горяинова, В. С. Овчинского, Г. К. Синилова. М.: Инфра-М, 2006. 832 с.
5. *Новиков Д. А.* Методология управления. М.: Книжный дом «Либроком»/URSS, 2012. 128 с.
6. Social Science for Counterterrorosm. Putting the Pieces Together / Davis P. K., Cragin K., Editors. RAND Corporation, 2009.
7. *Wilner A.* Cold War notion of deterrence works against terrorism, researcher contends // Journal of Strategic Studies http://www.vancouversun.com/news/Cold+notion+deterrence+works+against+terrorism+researcher+contends/4289343/story.html (дата обращения 10.03.2012)
8. *Wright P. D., Liberatore M. J., Nydick R. L.* A Survey of Operations Research Models and Applications in Homeland Security / Interfaces, 2006. V. 36, No 6, pp. 514–529.
9. *Sullivan T. J., Perry W. L.* Identifying indicators of chemical, biological, radiological, and nuclear (CBRN) weapons development activity in sub-national terrorist groups / J. Oper. Res. Soc., 2004, No 55(4), pp. 361–374.
10. *Pate-Cornell E.* Fusion of intelligence information: A Bayesian approach / Risk Anal. 2002, No 22(3), pp. 445–454.
11. *Каталевский Д. Ю.* Основы имитационного моделирования и системного анализа в управлении: учебное пособие. М.: Изд-во Московского университета, 2011. 304 с.
12. *Pita J., Jain M., Western C., Portway C., Tambe M., Ordonez F., Kraus S., Paruchuri P.* Deployed ARMOR protection: The application of a game theoretic model for security at the Los Angeles International Airport / In Proc. of AAMAS, 2008.
13. *Taylor M. E., Kiekintveld C., Western C., Tambe M.* Beyond Runtimes and Optimality: Challenges and Opportunities in Evaluating Deployed Security Systems / In Proceedings of the AAMAS-09 Workshop on Agent Design: Advancing from Practice to Theory, May 2009.

[7] Фьючерс — это программная конструкция, указывающая на то, что результат некоторого вычисления будет использоваться в программе позже, но само вычисление может планироваться системой в любой произвольный момент времени.

14. *Pita J., Tambe M., Kiekintveld C., Cullen S., Steigerwald E.* GUARDS-Game Theoretic Security Allocation on a National Scale / In Proc. of AAMAS, 2011, pp. 37–44.
15. *Новиков Д. А.* Иерархические модели военных действий / Управление большими системами. Вып. 37. М.: ИПУ РАН, 2012. С. 25–62.
16. Криминология: учебник для вузов / Под ред. д. ю. н., проф. А. И. Долговой. 3-е изд., перераб. и доп. М.: Норма, 2005. 912 с.
17. *Bachrach Y., Draief M., Goyal S.* Security games with contagion / University of Cambridge, 2011.
18. *Bier V., Oliveros S., Samuelson L.* Choosing what to protect: Strategic defensive allocation against an unknown attacker // Journal of Public Economic Theory, 2006, No 9, pp. 1–25.
19. *Kiekintveld C., Tambe M., Marecki J.* Robust Bayesian Methods for Stackelberg Security Games / Conference: Autonomous Agents & Multiagent Systems/Agent Theories, Architectures, and Languages — ATAL, pp. 1467–1468, 2010.
20. *Brynielsson J., Arnborg S.* Bayesian games for threat prediction and situation analysis / In FUSION, 2004.
21. *Arce D., Kovenock D., Roberson B.* Suicide terrorism and the weakest link, 2009.
22. *Golany B., Kaplan E., Marmur A., Rothblum U. G.* Nature plays with dice — terrorists do not: Allocating resources to counter probabilistic and strategic risks / European Journal of Operational Research, accepted September Vol. 192, pp. 198–208, 2009.
23. *Feinstein J. S., Kaplan E. H.* Analysis of a Strategic Terror Organization // Journal of Conflict Resolution, 2010. V. 54, issue 2, pp. 281–302.
24. *Caulkins J. P., Feichtinger G., Grass D., Tragler G.* Optimal control of terrorism and global reputation: A case study with novel threshold behavior / Operation Research Letters, No 37 (2009), pp. 387–391.
25. *Stranlund J. K., Field B. C.* On the Production of Homeland Security Under True Uncertainty / University of Massachusetts Amherst, Department of Resource Economics, Working Paper No 2006–5.
26. Control #7272, Why crime doesn't pay: Locating criminals through geographic profiling / Mathematical Contest in Modeling, University of Washington.
27. *Rossmo D. K.* Geographic profiling: Target Patterns of Serial Murderers / PhD thesis, Simon Fraser University, 1995.
28. *Shakarian P., Dickerson J., Subrahmanian V.* Adversarial Geospatial Abduction Problems. ACM Transactions on Intelligent Systems and Technology (TIST). 2012, 3(2), 34 : 1–34:35.
29. *Reed B.* A Social Network Approach to Understanding an Insurgency. Parameters, Summer, 2007, pp. 19–30.
30. *Shakarian P., Subrahmanian V. S., Sapino M. L.* SCARE: A Case Study with Baghdad — ICCCD, 2009.
31. *Shakarian P., Nagel M. K., Schuetzle B. E., Subrahmanian V. S.* Abductive Inference for Combat: Using SCARE-S2 to Find High-Value Targets in Afghanistan / Proceedings of the Twenty-Third Innovative Applications of Artificial Intelligence Conference, 2011. pp. 1689–1694.
32. *Shieh E.; An B.; Yang R.; Tambe M.; Baldwin C.; DiRenzo J.; Maule B.; and Meyer G.* 2012. PROTECT: A deployed game theoretic system to protect the ports of the United States. In Proc. of The 11 th International Conference on Autonomous Agents and Multiagent Systems (AAMAS).
33. *Ariely G. Bijak J. Landesmann R. Poria Y. and Warnes R.* (2011) Futures of Borders: A Forward Study of European Border Checks. Report for Frontex: EU external borders agency. Liron Systems Ltd./University of Southampton/University of Ben Gurion, Eilat/Southampton/ Be'er Sheva, December 2011.

Шумов Владислав Вячеславович. Доцент Отделения погранологии Международной академии информатизации. К. т. н. Окончил Военную академию им. М. И. Калинина в 1990 г. и МГУ в 1994 г. Количество печатных статей: более 50. Область научных интересов: погранология и погранометрика. E-mail: vshum59@yandex.ru