

УДК 323.28:519.876.2

**Шумов В.В.**

Модели противодействия терроризму: обзор

Шумов Владислав Вячеславович, кандидат технических наук, доцент, действительный член Отделения погранологии Международной академии информатизации.

E-mail: vshum59@yandex.ru

В статье приведен краткий обзор современных работ по моделированию системы противодействия терроризму и(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; убийства².

Классификация моделей противодействия терроризму

Классификация моделей по уровню абстракции / конкретности³: концептуальные модели, модели анализа и синтеза, реализация.

Концептуальные модели – разрабатываются специалистами предметной области, политологами, психологами, социологами и др. В качестве примера можно привести работу «Social Science for Counterterrorism. Putting the Pieces Together»⁴. 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, то есть 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

¹ FMFM 7-14 Combating Terrorism (USMC), 5 October 1990.

² Ibid.

³ Новиков Д.А. Методология управления. М.: Книжный дом «ЛИБРОКОМ», 2012. С. 26.

⁴ Social Science for Counterterrorism. Putting the Pieces Together. Davis P.K., Cragin K. (Editors). RAND Corporation, 2009.

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 информации¹: агентурная разведка; радиотехническая разведка; фоторазведка; анализ типовых операций.

А. Уилнер в статье «Понятие сдерживания времен холодной войны работает против терроризма» отмечает²: 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. По мнению Уилнера, включение теории сдерживания в войну с терроризмом путем ослабления соотношения затрат к выгоде в вопросе осуществления атаки, позволит заблаговременно манипулировать поведением террористических групп.

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»³. Модели классифицированы по следующим 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 охарактеризованы и классифицированы более 60-ти работ. В частности, Т. J. Sullivan и W. L. Perry⁴ 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.

Е. Pate-Cornell⁵ с использованием байесовского анализа разработал метод ранжирования угроз и назначения приоритетов мерам безопасности и объектам.

Технологии и документы, созданные на основе моделей (реализация). Руководство⁶ силами морской пехоты флота «Борьба с терроризмом» требует изменять шаблоны действий антитеррористических и военных подразделений с целью дезориентации террористов и повышения их риска. Рекомендуются 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.).

Названным Руководством, в частности, предусматривается следующая программа обучения по терроризму:

- Инструкция по пониманию угрозы (оценка угрозы, тактика террористов, безопасность места жительства и передвижений, защита от взрывных устройств);
- Инструкция по борьбе с терроризмом и вялотекущими конфликтами;
- заочные курсы по терроризму;
- группы мобильной подготовки от различных внешних организаций;
- специализированная подготовка и образование по терроризму.

В соответствии с федеральным законом⁷ противодействие терроризму включает следующие направления деятельности:

- предупреждение терроризма, в том числе 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.

Концепция⁸ противодействия терроризму в Российской Федерации определяет основную форму пресече-

¹ FMFM 7-14...

² Wilner A. Cold War notion of deterrence works against terrorism, researcher contends // Journal of Strategic Studies: <http://www.vancouversun.com>.

³ Wright P. D., Liberatore M. J., Nydick R. L. (2006). A Survey of Operations Research Models and Applications in Homeland Security // Interfaces. Vol. 36. No. 6. Pp. 514-529.

⁴ Sullivan T. J., Perry W. L. (2004). Identifying indicators of chemical, biological, radiological, and nuclear (CBRN) weapons development activity in sub-national terrorist groups / J. Oper. Res. Soc. No. 55(4). Pp. 361-374.

⁵ Pate-Cornell E. (2002). Fusion of intelligence information: A Bayesian approach // Risk Anal. No. 22(3). Pp. 445-454.

⁶ FMFM 7-14...

⁷ Федеральный закон от 06.03.2006 № 35-ФЗ (ред. от 08.11.2011) «О противодействии терроризму» // Официальный сайт компании "Консультант Плюс". [Электронный ресурс]. Режим доступа: <http://www.consultant.ru/popular/terror/>

⁸ Концепция противодействия терроризму в Российской Федерации. Утверждена Президентом Российской Федерации Д. Медведевым 5 октября 2009 г. // Российская газета. Федеральный выпуск № 5022, 20 октября 2009 г.

ния 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 деятельности¹ для борьбы с терроризмом могут использоваться следующие формы и виды оперативно-розыскных мероприятий: личный сыск², оперативный эксперимент³, оперативная комбинация⁴, оперативный поиск⁵, оперативная разработка⁶ и др.

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).

Руководством⁷ 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;
- *сигнальная безопасность* (signal security) – общий термин, охватывающий понятия «безопасность средств связи» и «безопасность электронных средств»;
- *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.

Некоторые модели находят практическое применение и встраиваются в программное обеспечение. Одно из важнейших требований к моделям – учет большого количества факторов.

По оценке Д. Ю. Каталевского⁸ модели, отвечающие запросам руководителей, обычно включают от 30 до 3000 переменных. Нижний предел близок к тому минимуму, который отражает основные типы поведения системы, интересные тех, кто принимает решения. Верхний предел ограничивается нашими возможностями восприятия системы и всех ее взаимосвязей.

В этой связи на практике обычно используются комплексные модели с параметрами, измеренными в различных шкалах. Рассмотрим теоретико-игровую модель⁹ для обеспечения безопасности в международном аэропорту г. Лос-Анджелес, 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.

¹ Теория оперативно-розыскной деятельности: учебник / Под ред. К.К. Горяинова, В.С. Овчинского, Г.К. Синилова. М.: ИНФРА-М, 2006. 832 с.

² Личный сыск – обнаружение, выявление, поиск, розыск, осуществляемое лично субъектом этих действий.

³ Оперативный эксперимент – воспроизведение действий, обстановки или иных обстоятельств противоправного события и совершение необходимых опытных.

⁴ Оперативная комбинация – комплекс действий, объединенных единым замыслом, легендой и направленных на решение конкретной задачи обнаружения, предотвращения или раскрытия преступления.

⁵ 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.

⁶ 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.

⁷ FMFM 7-14 ...

⁸ Каталевский Д. Ю. Основы имитационного моделирования и системного анализа в управлении. Учебное пособие. М.: Изд-во Московского университета, 2011.

⁹ Pita J., Jain M., Western C., Portway C., Tambe M., Ordóñez F., Kraus S., Paruchuri P. (2008). Deployed ARMOR protection: The application of a game theoretic model for security at the Los Angeles International Airport / In Proc. of AAMAS.

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 года. М. Taylor и др. описали тесты для его проверки¹:

- 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 работе². Основные проблемы:

- сотни разнородных пунктов охраны;
- разнообразие угроз;
- частично централизованный подход к обучению персонала и развитию системы.

Классификация моделей системы противодействия терроризму. В настоящем подразделе перечислены некоторые возможные основания для классификации.

Первое основание для классификации моделей – по направлениям деятельности:

- модели профилактики (предупреждения)³ терроризма;
- модели сдерживания терроризма;
- модели предотвращения терроризма;
- модели пресечения террористической деятельности;
- модели прогнозирования угроз;
- модели минимизации и (или) ликвидации последствий проявлений терроризма.

Второе основание для классификации моделей – по масштабу контртеррористических систем:

- модели уровня подразделения;
- модели уровня региона;
- модели уровня ведомства;
- модели межведомственного уровня;
- модели уровня государства (общества);
- модели межгосударственного уровня.

Третье основание для классификации – 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.

Четвертое основание для классификации – 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.

Пятое основание для классификации – по видам террористических организаций:

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

Шестое основание для классификации – по мотивации:

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

¹ Taylor M. E., Kiekintveld C., Western C., Tambe M. (2009). 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.

² Pita J., Tambe M., Kiekintveld C., Cullen S., Steigerwald E. (2011). GUARDS - Game Theoretic Security Allocation on a National Scale / In Proc. of AAMAS. Pp. 37–44.

³ В широком понимании профилактика является синонимом предупреждения. В узком смысле слова профилактикой считаются меры, направленные на выявление и ликвидацию причин и условий конкретных деяний, а также на установление лиц, способных совершить преступление, с целью осуществления направленного предупредительного воздействия (Аванесов Г. А. Криминология. Учебник, 2-е изд., перераб. и доп. М.: Изд-во Акад. МВД СССР, 1984. С. 339).

- модели противодействия терроризму с криминальной мотивацией.

Седьмое основание для классификации – по методу моделирования:

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

Теоретико-игровые модели борьбы с терроризмом относятся к классу Security Game¹. Их можно найти в экономических, политических, компьютерных и иных исследованиях. Одно из решений – моделирование в области безопасности на основе байесовских игр², в которых полагается известным распределение противника по типам. В некоторых работах для поиска оптимальных стратегий сторон используется игра полковника Блотто³. К сожалению, в них не учитывается очевидный факт, что противник способен вести наблюдение за системой охраны и использовать эту информацию.

Боуз Голэни и др.⁴ 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»⁵ моделируют выбор террористическими организациями масштаба и горизонта планирования террористических атак и влияние последствий этого выбора на развитие организаций.

Д. Калкинс и др.⁶ рассматривают модель оптимального управления борьбы с терроризмом, учитывающую уровень общественных симпатий к антитеррористическим силам.

Теоретико-игровой подход к моделированию противодействия терроризму

Теория игр – это раздел прикладной математики, исследующий модели принятия решений в условиях несовпадения интересов сторон (игроков), когда каждая сторона стремится воздействовать на развитие ситуации в собственных интересах⁷.

Теоретико-игровые модели обеспечения безопасности (Security Games) обычно рассматривают конфликтные ситуации между защитником (лидером, центром) и одним или несколькими атакующими (агентами, террористами).

Функции технологии конфликта (contest success function, CSF). Функции технологии конфликта подразделяются на два класса: соотношения сил (ratio function) и разницы сил (difference function).

Пусть имеется множество $N = \{1, \dots, n\}$ целей (объектов), которые могут быть атакованы. Обозначим через $x = (x_1, \dots, x_n)$ – действие защитника, через $q = (q_1, \dots, q_n)$ – действие атакующего, где $x_i \geq 0$ ($q_i \geq 0$) – количество бесконечно делимого ресурса, выделенного защитником (атакующим) на объект $i = 1, \dots, n$. Ценность i -го объекта для защитника (атакующего) обозначим через X_i (Q_i). На ресурсы наложены ограничения:

$$\sum_{i \in N} x_i \leq R_x, \quad \sum_{i \in N} q_i \leq R_y. \quad (1)$$

При использовании функции соотношения сил вероятность победы защитника на объекте i пропорциональна количеству выделенного на этот объект ресурса и обратно пропорциональна взвешенной сумме ресурсов, выделенными на этот объект обоими игроками⁸:

$$p_x(x_i, q_i) = \frac{\alpha_i (x_i)^{r_i}}{\alpha_i (x_i)^{r_i} + (q_i)^{r_i}}, \quad r_i \in (0; 1], \alpha_i > 0, \quad p_x(0, 0) = \frac{\alpha_i}{\alpha_i + 1}, \quad (2)$$

где α_i характеризует соотношение эффективностей использования игроками ресурсов на объекте i , r_i – отражает решительность (эффективность) конфликта⁹.

Соответственно, вероятность победы атакующего на объекте i равна:

$$p_q(x_i, q_i) = 1 - p_x(x_i, q_i). \quad (3)$$

¹ Bachrach Y., Draief M., Goyal S. (2011). Security games with contagion. Tech. Rep.

Bier V., Oliveros S., Samuelson L. (2006). Choosing what to protect: Strategic defensive allocation against an unknown attacker // Journal of Public Economic Theory. No. 9. Pp. 1-25.

Kiekintveld C., Tambe M., Marecki J. (2010). Robust Bayesian Methods for Stackelberg Security Games // Conference: Autonomous Agents & Multiagent Systems/Agent Theories, Architectures, and Languages. ATAL. pp. 1467-1468.

² Brynielsson J., Arnborg S. (2004). Bayesian games for threat prediction and situation analysis. In International Conference on Information Fusion (FUSION).

³ Arce D., Kovenock D., Roberson B. (2009). Suicide terrorism and the weakest link, APSA 2009 Toronto Meeting Paper. Available at SSRN: <http://ssrn.com/abstract=1449856>.

⁴ Golany B., Kaplan E., Marmur A., Rothblum U.G. (2009). Nature plays with dice – terrorists do not: Allocating resources to counter probabilistic and strategic risks // European Journal of Operational Research. Vol. 192. Pp. 198–208.

⁵ Feinstein J.S., Kaplan E.H. (2010). Analysis of a Strategic Terror Organization // Journal of Conflict Resolution. Vol. 54. Issue 2. Pp. 281–302.

⁶ Caulkins J.P., Feichtinger G., Grass D., Tragler G. (2009). Optimal control of terrorism and global reputation: A case study with novel threshold behavior // Operation Research Letters. No 37. Pp. 387–391.

⁷ Воробьев Н.Н. Основы теории игр. Бескоалиционные игры. М.: Наука, 1984. 495 с.

⁸ Новиков Д.А. Иерархические модели военных действий // Управление большими системами. Вып. 37. М.: ИПУ РАН, 2012. С. 25–62.

⁹ Garfinkel M., Skaperdas S. (2006). Economics of conflict: An Overview. In T. Sandler and K. Hartley (Eds.), Handbook of Defense Economics. Chapter 3. 65 p.

Если количество ресурсов измеряется в людских единицах, то параметр α_i содержательно означает отношение боевых потенциалов защитника и атакующего. Причем это отношение зависит не только от вооружения и экипировки участников конфликта, но и от способов тактических действий. Находясь в обороне, субъект, при прочих равных условиях, обычно (но не всегда) имеет боевое преимущество перед наступающим¹. Например, находясь в засаде, террористы обстреливают колонну автомашин.

Вероятность победы лидера может вычисляться и с использованием логит-модели² (функция разности сил):

$$p_x(x_i, q_i) = \frac{\exp(kx_i)}{\exp(kx_i) + \exp(kq_i)} = \frac{1}{1 + \exp(k(q_i - x_i))}, \quad k > 0. \quad (4)$$

При использовании выражений (2–4) предполагается, что бой продолжается до полного уничтожения одной из сторон, то есть ничья считается почти невозможным исходом. К тому же в данных выражениях не учитывается известный из военной теории факт, что одна из сторон выходит из боя при достижении определенного уровня потерь³. В частности, небоеспособными признаются части и подразделения при наличии в них менее 40% боевого состава⁴.

В играх безопасности использование выражений (2–4) разумно, поскольку обычно нападение террористов на некоторый объект заканчивается или успехом, или неудачей. Вместе с тем, могут быть ситуации, когда после атаки стороны оказываются в том же состоянии, что и до нее. То есть ничья является разумным выходом из тупика. Для фиксации подобных возможностей вводится следующие функции конфликта:

$$p_x(x_i, q_i) = \frac{f_x(x_i, q_i)}{1 + f_x(x_i, q_i) + f_q(x_i, q_i)}, \quad p_q(x_i, q_i) = \frac{f_q(x_i, q_i)}{1 + f_x(x_i, q_i) + f_q(x_i, q_i)}, \quad (5)$$

где $f_x(\cdot)$ и $f_q(\cdot)$ неотрицательные возрастающие функции.

Единицу в знаменателе можно рассматривать как участие в игре третьей стороны – «природы». При использовании данных функций вероятность ничейного исхода всегда положительна:

$$1 - p_x(x_i, q_i) - p_q(x_i, q_i) = \frac{1}{1 + f_x(x_i, q_i) + f_q(x_i, q_i)}. \quad (6)$$

Игра полковника Блотто. Если террористы не изучают систему охраны объектов (или отсутствуют возможности для изучения в связи со скрытыми действиями охраны), имеется только один террорист (одна группа), то можно считать, что оба игрока однократно и одновременно распределяют свои ограниченные ресурсы по объектам. Выигрыши игроков в вероятностной модели вычисляются по формулам:

$$F_x(x, q) = \sum_{i \in N} p_x(x_i, q_i), \quad F_q(x, q) = \sum_{i \in N} p_q(x_i, q_i). \quad (7)$$

При ограниченном числе объектов n и для случая $X_i = Q_i = \text{Const}$, $r_i = 1$, $\alpha_i = 1$, $i \in N$, $R_x \neq R_y$ единственным равновесием Нэша (решением игры) является использование игроками чистых стратегий, заключающихся в равном распределении имеющихся у них ресурсов между объектами.

Иерархическая игра защитник – атакующие (охрана Лос-анджелесского аэропорта). Рассмотрим описание игры, которая реализована в системах поддержки принятия решений (охрана аэропортов, служба воздушных маршалов, береговая охрана). Задача – найти оптимальную смешанную стратегию защитника в предположении, что атакующие, возможно, знают эти стратегии и учитывают их при выборе своих действий.

Формальная постановка задачи⁶:

$$\begin{aligned} \max_{x, q, a} \sum_{i \in X} \sum_{l \in L} \sum_{j \in Q} p^l R_{ij}^l x_i q_j^l, \\ \sum_{i \in X} x_i = 1, \quad \sum_{j \in Q} q_j^l = 1, \quad 0 \leq \left(a^l - \sum_{i \in X} C_{ij}^l x_i \right) \leq (1 - q_j^l) M, \\ x_i \in [0 \dots 1], \quad q_j^l \in \{0, 1\}, \quad a \in \mathfrak{R}, \end{aligned} \quad (8)$$

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

q^l – вектор-стратегия атакующего типа l ;

R^l и C^l – матрицы выигрышей защитника и атакующего типа l ;

M – большое положительное число;

p^l – априорная вероятность атакующего типа l .

Первое и четвертое ограничения определяют множество возможных действий защитника как распределение вероятностей на множестве X . Второе и пятое ограничения определяют множество возможных действий

¹ Ibid.

² Ibid.

³ Головин Н.Н. Наука о войне. О социологическом изучении войны. Париж: Издательство газеты «Сигнал», 1938.

⁴ Война и мир в терминах и определениях. Под общей ред. Д.О. Рогозина. М.: Изд. дом «ПоРог», 2004.

⁵ Garfinkel M., Skaperdas S. (2006). Oh. Cit.

⁶ Pita J., Jain M., Western C., Portway C., Tambe M., Ordonez F., Kraus S., Paruchuri P. (2008). Deployed ARMOR protection: The application of a game theoretic model for security at the Los Angeles International Airport. In Proc. of AAMAS. Pp. 125–132.

атакующего типа l . Каждый атакующий l имеет строго одну единичную стратегию. Третье ограничение работает следующим образом:

левая часть неравенства означает, что a^l есть верхняя граница выигрыша атакующего l ;

для действия $q_j^l = 1$ правая часть неравенства означает, что это действие должно быть оптимальным для атакующего l .

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

Если защитник выбрал дорогу i для проверки, а атакующий l – дорогу j , то защитник получает вознаграждение R_{ij}^l , а атакующий – C_{ij}^l . Если защитник задерживает атакующего, то его выигрыш положителен, а выигрыш атакующего отрицателен. Интенсивность потока машин на дорогах и ценность этих дорог для атакующих учитываются посредством назначений значений выигрышей.

Заменой $z_{ij}^l = x_i q_j^l$ задача (8) сводится к задачам целочисленного линейного программирования.

Особенности игр безопасности с ограниченной рациональностью игроков. В силу различных причин (недостаток информации, нежелание производить вычисления и т.д.) игроки характеризуются ограниченной рациональностью. Для учета в моделях ограниченной рациональности используется теория перспектив¹ и равновесие дискретного выбора² (Quantal response equilibrium – QRE).

В теории перспектив вместо функции полезности вычисляется *ожидаемая стоимость* или так называемая перспектива:

$$\sum_{i=1}^k \pi_i^-(p_i) U(x_i) + \sum_{j=k+1}^n \pi_j^+(p_j) U(x_j), \quad x_1 \leq \dots \leq x_k \leq 0 \leq x_{k+1} \leq \dots \leq x_n, \quad (9)$$

где: p_i – вероятность получения результата x_i ,

$\pi^+(\cdot)$ и $\pi^-(\cdot)$ – весовая функция дохода и потерь, описывающая, как воспринимается вероятность p_i ,

$U(\cdot)$ – функция стоимости, отражающая восприятие результата, $U(0) = 0$.

Для нахождения равновесия дискретного выбора с использованием логит-модели вычисляются вероятности выбора атакующим цели i :

$$q_i(t_i) = \frac{\exp(\lambda U_a^c(t_i))}{\sum_{k=1, \dots, n} \exp(\lambda U_a^c(t_k))}, \quad (10)$$

где $\lambda \geq 0$ – степень рациональности атакующего.

Цель защитника – максимизация своей функции полезности U_d при известной смешанной стратегии атакующего. Поиск равновесий выполняется численными методами.

Игры безопасности на сетях и графах. В играх безопасности используются конструкции и результаты теории графов:

- структура принятия решений в игре безопасности в развернутой форме задается древовидным графом³;
- выявление террористической группы по телефонным вызовам с использованием моделей анализа социальной сети⁴;
- на графе в дискретном времени осуществляются игры поиска и игры патрулирования⁵ и т.д.

С конца 1970-х гг. прошлого века развивается теория сетевых игр (network games) – раздел теории игр, акцентирующий внимание на формировании сетевых структур – устойчивых связей между игроками – в условиях несовершенства интересов и/или различной информированности последних⁶.

Игры на сетях подразделяются на⁷:

- игры маршрутизации (networking games);
- «когнитивные игры» (cognitive maps games);
- игры на социальных сетях (social networks games);
- игры на сетевых графиках.

В играх безопасности, поиска и патрулирования на графах рассматривается игра на графе $Q = (N, E)$, где N – множество вершин ($N = \{1, 2, \dots, n\}$), E – множество дуг. Временной период цикла игры разбивается на дискретные периоды $t = 1, \dots, T$.

¹ Booij A., Praag B., Kuilen G. (2009). A Parametric Analysis of Prospect Theory's Functionals for the General Population // IZA DP. No. 4115.

² McKelvey R. D., Palfrey T. R. (1995). Quantal response equilibria for normal form games. Games and Economic Behavior. No. 2. Pp. 6–38.

³ Feinstein J.S., Kaplan E.H. (2010). Analysis of a Strategic Terror Organization // Journal of Conflict Resolution. Vol. 54. Issue 2. Pp. 281–302.

⁴ Azad, S., Gupta, A. (2011). A Quantitative Assessment on 26/11 Mumbai Attack using Social Network Analysis // Journal of Terrorism Research, North America, No. 2.

⁵ Agmon N., Kraus S., Kaminka G. A. (2008). Multi-robot perimeter patrol in adversarial settings. In ICRA, Pp. 2339–2345.

⁶ Новиков Д.А. Игры и сети // Математическая теория игр и ее приложения. Т. 2. Вып. 1. Петрозаводск: КарНЦ РАН, 2010. С. 107–124.

⁷ Там же. С. 109.

Атакующий выбирает для атаки узел i и стадию τ . Атакующий действует m периодов ($m \leq T$). Его смешанная стратегия – $p(i, \tau)$. Защитник выбирает маршрут w патрулирования продолжительностью T периодов и его действия считаются успешными, если выполняется перехват атакующего. Смешанная стратегия защитника – $p(w)$.

На рис. 1 показан пример игры патрулирования¹ при $n = 5$, $T = 8$, $m = 4$ (атакующий – пунктирная линия, защитник – сплошная).

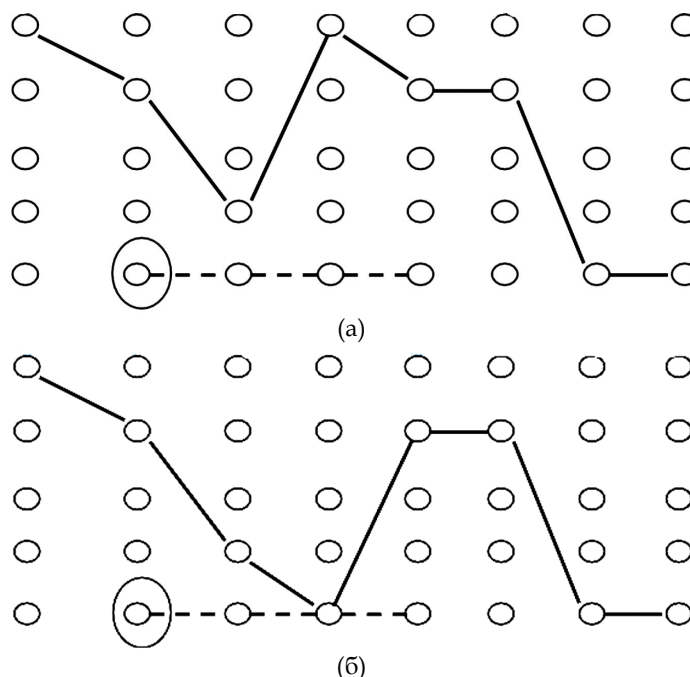


Рис. 1. Игра патрулирования: (а) атака успешна, (б) – неуспешна

В случае (а) маршрут защитника: $w = 1-2-4-1-2-2-5-5$, маршрут атакующего: $(i, \tau) = (5, 2)$. Маршруты не пересекались, что свидетельствует об успешности атаки. В случае (б): $w = 1-2-4-5-2-2-5-5$, $(i, \tau) = (5, 2)$; атака неуспешна.

Игра патрулирования с нулевой суммой в нормальной форме записывается в виде $G(Q, T, m)$ с выигрышем защитника (вероятностью перехвата атакующего) $V(Q, T, m)$. В статье «Patrolling games» приведены аналитические выражения функции выигрыша для графов различных типов.

В работе «Computing Time-Dependent Policies for Patrolling Games with Mobile Targets»² рассматривается игра между защитником и одним атакующим на ориентированном графе. Задача мобильного защитника – патрулирование территории, на которой расположены подвижные или неподвижные объекты, представляющие интерес для нападающих. Район патрулирования представляется графом с произвольной топологией. Атакующий способен вести наблюдение за действиями защитника. Авторами построена теоретико-игровая формулировка задачи и найдены оптимальные стратегии сторон.

Первоначально для решения подобных задач использовались игры патрулирования периметра³, но они мало применимы в среде с более общей топологией.

Игры класса Border Game и Barrier Game. В борьбе с трансграничным терроризмом важная роль отводится пограничным службам. Существует класс игровых задач (Border Game), предназначенных для поиска оптимальных стратегий пограничных формирований.

Л. Вейн и А. Мотскин в статье «Анализ национальной безопасности США – мексиканская граница»⁴ описали оптимизационную теоретико-игровую модель, позволяющую минимизировать вероятность безнаказанного въезда на территорию США террористов. Модель включает в себя следующие подмодели:

- *подмодель выбора* – агенты (потенциальные нарушители границы) принимают решение о выборе альтернативы (нарушить границу или нет) исходя из максимизации ожидаемой полезности в условиях ограниченной рациональности. Авторами использовалась логит-модель, для которой они методом максимального правдоподобия нашли оценку параметра (степени рациональности агентов);

- *подмодель задержания* рассматривается как иерархическая игра, в которой первый шаг делает Правительство США, размещая некоторым образом силы и средства на границе. Подмодель позволяет учесть такти-

¹ Alpern S., Morton A., Papadaki K. (2011). Patrolling games // Operations research. No. 59 (5). Pp. 1246–1257.

² Bosansky B., Lisy V., Jakob M., Pechoucek M. (2011). Computing Time-Dependent Policies for Patrolling Games with Mobile Targets // In Tenth International Conference on Autonomous Agents and Multiagent Systems (to appear). Pp. 989–996; Amigoni F., Basilico N., Gatti N., Saporiti A., Troiani S. (2010). Moving game theoretical patrolling strategies from theory to practice: An USARSim simulation. ICRA. Pp. 426–431.

³ Agmon N., Kraus S., Kaminka G. A. (2008). Multi-robot perimeter patrol in adversarial settings. In ICRA, Pp. 2339–2345.

⁴ Wein L., Liu Y., Motskin A. (2009). Analyzing the Homeland Security of the U.S.-Mexico Border // Risk Analysis. Vol. 29. Issue 5. Pp. 699–713.

ку действий правительства, которая заключается в следующем: правительство будет перераспределять пограничные патрули на те участки, где недавно зафиксированы нарушения; в свою очередь нарушители будут уходить на менее охраняемые участки границы;

– *подмодель выдворения* задержанных нарушителей рассматривается как система массового обслуживания. Заявками системы являются задержанные нарушители или лица, получившие судебное предписание о выдворении (среди таковых только 13% реально выдворяются за пределы США);

– *подмодель рынка нелегального труда* основана на использовании производственной функции Кобба-Дугласа с двумя факторами (неквалифицированные рабочие и капитал).

В ходе расчетов при существующей технологии охраны границы (15% границы с Мексикой контролируются техническими средствами наблюдения, в каждый момент времени на границе несут службу 1636 пограничных патрулей) вероятность бесконтрольного преодоления границы потенциальными террористами равна примерно 0,973.

В связи с большой протяженностью границ и отсутствием возможности обеспечить их сплошное прикрытие нарядами (патрулями) и техническими средствами, важную роль в охране границы приобретают беспилотные летательные аппараты (БПЛА). Поиску оптимальных способов применения БПЛА в охране границы посвящен ряд работ¹.

БПЛА могут применяться и в ходе контртеррористических действий для контроля важных рубежей (Barrier Game). Эффективность БПЛА выше эффективности стационарных средств с такими же возможностями по обнаружению целей за счет наличия упреждающих и остаточных областей² (рис. 2).

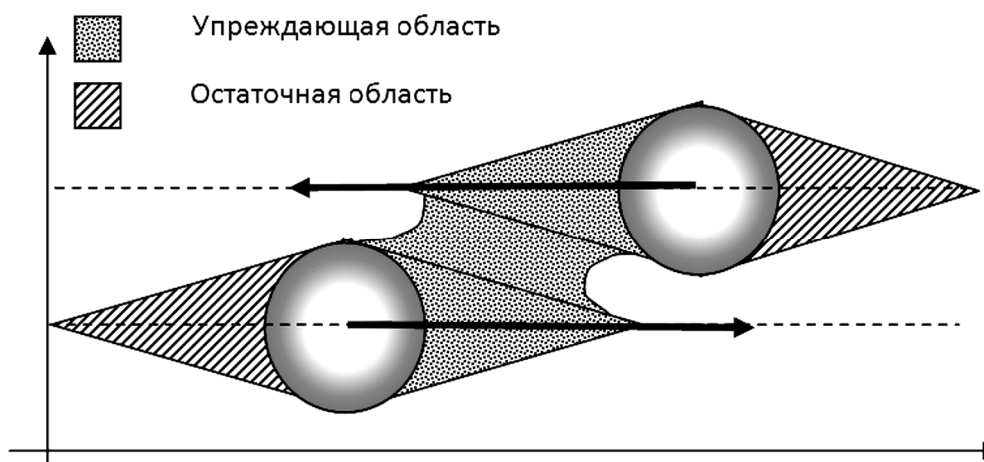


Рис. 2. Взаимодействие упреждающих областей поисковых систем

Если поисковая система (ПС) покоится, то ее осведомленность об искомом объекте (ИО) ограничивается кругом, центр которого совпадает с ПС. При движении ПС эта область увеличивается: впереди образуется *упреждающая область*, сзади – *остаточная область*. Объединение этих областей образует *следящую область*, показывающую степень осведомленности ПС об ИО.

Рефлексивные игры, информационное управление и борьба с терроризмом. Опыт боевых и специальных действий показывает, что добиться решающих успехов можно за счет повышения эффективности взаимодействия между участниками. В частности, Германия добивалась решающих успехов в военных компаниях второй мировой войны за счет применения блицкрига, идея которого заключалась в использовании танков во взаимодействии с авиацией и мотопехотой³. Блицкриг стал фактически новым организационным оружием. В терминологии теории игр блицкриг есть доминирующая стратегия. Современные сетевые операции⁴ характеризуются децентрализованностью взаимодействия. Прогноз поведения агентов в контртеррористической операции возможен с использованием теории рефлексивных игр⁵, в которой рассматривается:

– *информационная рефлексия* (процесс и результат размышлений агента о том, каковы значения неопределенных параметров, и что об этих значениях знают и думают его оппоненты);

– *стратегическая рефлексия* (процесс и результат размышлений агента о том, какие принципы принятия решений используют его оппоненты).

Методами рефлексивных игр могут в частности решаться задачи скрытого управления субъектами воздей-

¹ Kiekintveld C., Kreinovich V., Lerma O. (2011). Optimizing Trajectories for Unmanned Aerial Vehicles (UAVs) Patrolling the Border // Proceedings of the World Conference on Soft Computing, San Francisco, CA, May 23–26; Шумов В.В. Модели пограничного сдерживания. М.: ЛЕНАНД, 2012. 200 с.

² Чхартишвили А.Г., Шикин Е.В. Динамический поиск объектов. Геометрический взгляд на проблему // Фундаментальная и прикладная математика. 1995. Т. 1. № 4. С. 827–862; Шикин Е.В., Березин С.Б. Поиск объектов. Динамика. Геометрия. Графика // Фундаментальная и прикладная математика. 2005. Том 11. № 1. С. 3–34; Washburn A.R. (2010). Barrier Games // Military Operations Research. No 15(3). Pp. 31–41.

³ Алексеев В.В., Нефедов С.А. Технологическая интерпретация истории второй мировой войны. [Электронный ресурс]. Режим доступа: <http://book.uraic.ru>

⁴ Арзуманян Р. Теория и принципы сетевых войн и операций // 21-й ВЕК. № 2 (8), 2008. С. 66–127.

⁵ Новиков Д.А., Чхартишвили А.Г. Рефлексивные игры. М.: Синтег, 2003. 149 с.

ствия (террористы, пособники, заинтересованные лица, население и т.д.):

- информационные воздействия направлены на представления агента о среде:
 - моделирование несуществующей реальности;
 - представление настоящего ложным, а ложного настоящим;
- информационные воздействия направлены на представления агента о представлениях активного субъекта о среде:
 - навязывание агенту шаблона восприятия за счет проведения демонстративных действий, маскирующих действительную цель;
 - убеждение агента в том, что он правильно оценивает твои планы, и достижение результата нестандартным способом;
 - заставить агента недооценить твои возможности, способности и осведомленность и т.д.

Анализ информационных воздействий выполняется с использованием¹ марковских моделей, конечных автоматов, моделей диффузии инноваций, моделей заражения и др. Для решения некоторых задач информационного управления могут использоваться аксиомы представления субъектов о параметрах среды и оппонентов².

Продолжение следует

ЛИТЕРАТУРА

1. Федеральный закон от 06.03.2006 № 35-ФЗ (ред. от 08.11.2011) «О противодействии терроризму» // Официальный сайт компании «Консультант Плюс». [Электронный ресурс]. Режим доступа: <http://www.consultant.ru/popular/terror/>
Federal'nyi zakon ot 06.03.2006 № 35-FZ (red. ot 08.11.2011) «O protivodeistvii terrorizmu». Ofitsial'nyi sait kompanii "Konsul'tant Plus". URL: <http://www.consultant.ru/popular/terror/>
2. Концепция противодействия терроризму в Российской Федерации. Утверждена Президентом Российской Федерации Д. Медведевым 5 октября 2009 г. // Российская газета. 2009. 20 октября. Федеральный выпуск № 5022. Kontseptsiya protivodeistviya terrorizmu v Rossiiskoi Federatsii. Utverzhdena Prezidentom Rossiiskoi Federatsii D. Medvedevym 5 oktyabrya 2009 g. Rossiiskaya gazeta. 2009. 20 oktyabrya. Federal'nyi vypusk № 5022.
3. Аванесов Г. А. Криминология. Учебник, 2-е изд., перераб. и доп. М.: Изд-во Акад. МВД СССР, 1984. Avanesov G.A. (1984). Kriminologiya. Uchebnik, 2-e izd., pererab. i dop. Izd-vo Akad. MVD SSSR. Moskva. 526 p.
4. Алексеев В.В., Нефедов С.А. Технологическая интерпретация истории второй мировой войны. [Электронный ресурс]. Режим доступа: <http://book.uraic.ru>
Alekseev V.V., Nefedov S.A. Tehnologicheskaya interpretatsiya istorii vtoroi mirovoi voyny. URL: <http://book.uraic.ru>
5. Арзуманян Р. Теория и принципы сетцентричных войн и операций // 21-й ВЕК. № 2 (8), 2008. С. 66–127. Arzumanyan R. (2008). Teoriya i principy setetsentrichnykh voyn i operatsii. 21-i VEK. N 2 (8), Pp. 66–127.
6. Война и мир в терминах и определениях. Под общей ред. Д.О. Рогозина. М.: Изд. дом «ПоРог», 2004. Voyna i mir v terminakh i opredeleniyakh: pod obshchei red. D.O. Rogozina. Izd. dom "PoRog", Moskva. 2004. 624 p.
7. Воробьев Н.Н. Основы теории игр. Бескоалиционные игры. М.: Наука, 1984. 495 с. Vorob'ev N.N. (1984). Osnovy teorii igr. Beskoalitsionnye igry. Nauka. Moskva. 495 p.
8. Головин Н.Н. Наука о войне. О социологическом изучении войны. Париж: Издательство газеты «Сигнал», 1938. Golovin N.N. (1938). Nauka o voine. O sotsiologicheskom izuchenii voyny. Izdatel'stvo gazety «Signal». Parizh.
9. Губанов Д.А., Новиков Д.А., Чхартишвили А.Г. Социальные сети: модели информационного влияния, управления и противоборства. М.: Физматлит, 2010. 244 с. Gubanov D.A., Novikov D.A., Chkhartishvili A.G. (2010). Social'nye seti: modeli informatsionnogo vliyaniya, upravleniya i protivoborstva. Fizmatlit, Moskva. 244 p.
10. Каталевский Д.Ю. Основы имитационного моделирования и системного анализа в управлении. Учебное пособие. М.: Изд-во Московского университета, 2011. Katal'evskii D.Yu. (2011). Osnovy imitatsionnogo modelirovaniya i sistemnogo analiza v upravlenii. Uchebnoe posobie. Izd-vo Moskovskogo universiteta, Moskva.
11. Новиков Д.А. Игры и сети // Математическая теория игр и ее приложения. Т. 2. Вып. 1. Петрозаводск: КарНЦ РАН, 2010. С. 107–124. Novikov D.A. (2010). Igry i seti. Matematicheskaya teoriya igr i ee prilozheniya. T. 2. Vyp. 1. KarNTs RAN. Petrozavodsk. Pp. 107–124.
12. Новиков Д.А. Иерархические модели военных действий // Управление большими системами. Вып. 37. М.: ИПУ РАН, 2012. С. 25–62. Novikov D.A. (2012). Ierarkhicheskie modeli voennykh deistvii. Upravlenie bol'shimi sistemami. Vyp. 37. IPU RAN. Moskva. Pp. 25–62/
13. Новиков Д.А. Методология управления. М.: Книжный дом «ЛИБРОКОМ», 2012. Novikov D.A. (2012). Metodologiya upravleniya. Knizhnyi dom «LIBROKOM», Moskva.
14. Новиков Д.А., Чхартишвили А.Г. Рефлексивные игры. М.: Синтег, 2003. 149 с. Novikov D.A., Chkhartishvili A.G. (2003). Refleksivnye igry. Sinteg, Moskva. 149 p.
15. Теория оперативно-розыскной деятельности: учебник / Под ред. К.К. Горяинова, В.С. Овчинского, Г.К. Синилова. М.: ИНФРА-М, 2006. 832 с. Teoriya operativno-rozysknoi deyatel'nosti: uchebnik. Pod red. K.K. Goryainova, V.S. Ovchinskogo, G.K. Sinilova. INFRA-M. Moskva. 2006. 832 p.
16. Чхартишвили А.Г., Шикин Е.В. Динамический поиск объектов. Геометрический взгляд на проблему //

¹ Губанов Д.А., Новиков Д.А., Чхартишвили А.Г. Социальные сети: модели информационного влияния, управления и противоборства. М.: Физматлит, 2010. 244 с.

² Шумов В.В. Модели пограничного сдерживания. С. 112–117.

- Фундаментальная и прикладная математика. 1995. Т. 1. № 4. С. 827–862.
- Chkhartishvili A.G., Shikin E.V. (1995). Dinamicheskii poisk ob"ektov. Geometricheskii vzglyad na problemu. Fundamental'naya i prikladnaya matematika. T. 1, N 4. Pp. 827–862.
17. Шикин Е.В., Березин С.Б. Поиск объектов. Динамика. Геометрия. Графика // Фундаментальная и прикладная математика. 2005. Том 11. № 1. С. 3–34.
Shikin E.V., Berezin S.B. (2005). Poisk ob"ektov. Dinamika. Geometriya. Grafika. Fundamental'naya i prikladnaya matematika. T. 11. N 1. Pp. 3–34.
18. Шумов В.В. Модели пограничного сдерживания. М.: ЛЕНАНД, 2012. 200 с.
Shumov V.V. (2012). Modeli pogranichnogo sderzhivaniya. LENAND. Moskva. 200 p.
19. FMFM 7-14 Combating Terrorism (USMC), 5 October 1990.
20. Agmon N., Kraus S., Kaminka G. A. (2008). Multi-robot perimeter patrol in adversarial settings. In ICRA, Pp. 2339–2345.
21. Alpern S., Morton A., Papadaki K. (2011). Patrolling games // Operations research. No. 59 (5). Pp. 1246–1257.
22. Amigoni F., Basilico N., Gatti N., Saporiti A., Troiani S. (2010). Moving game theoretical patrolling strategies from theory to practice: An USARSim simulation. ICRA. Pp. 426–431.
23. Arce D., Kovenock D., Roberson B. (2009). Suicide terrorism and the weakest link, APSA 2009 Toronto Meeting Paper. Available at SSRN: <http://ssrn.com/abstract=1449856>.
24. Azad, S., Gupta, A. (2011). A Quantitative Assessment on 26/11 Mumbai Attack using Social Network Analysis // Journal of Terrorism Research, North America, No. 2.
25. Bachrach Y., Draief M., Goyal S. (2011). Security games with contagion. Tech. Rep.
26. Bier V., Oliveros S., Samuelson L. (2006). Choosing what to protect: Strategic defensive allocation against an unknown attacker // Journal of Public Economic Theory. No. 9. Pp. 1–25.
27. Booij A., Praag B., Kuilen G. (2009). A Parametric Analysis of Prospect Theory's Functionals for the General Population // IZA DP. No. 4115.
28. Bosansky B., Lisy V., Jakob M., Pechoucek M. (2011). Computing Time-Dependent Policies for Patrolling Games with Mobile Targets // In Tenth International Conference on Autonomous Agents and Multiagent Systems (to appear). Pp. 989–996.
29. Brynielsson J., Arnborg S. (2004). Bayesian games for threat prediction and situation analysis. In International Conference on Information Fusion (FUSION).
30. Caulkins J.P., Feichtinger G., Grass D., Tragler G. (2009). Optimal control of terrorism and global reputation: A case study with novel threshold behavior // Operation Research Letters. No 37. Pp. 387–391.
31. Feinstein J.S., Kaplan E.H. (2010). Analysis of a Strategic Terror Organization / Journal of Conflict Resolution. Vol. 54. Issue 2. Pp. 281–302.
32. Garfinkel M., Skaperdas S. (2006). Economics of conflict: An Overview / In T. Sandler and K. Hartley (Eds.), Handbook of De-fense Economics. Chapter 3. 65 p.
33. Golany B., Kaplan E., Marmur A., Rothblum U.G. (2009). Nature plays with dice – terrorists do not: Allocating resources to counter probabilistic and strategic risks / European Journal of Operational Research. Vol. 192. Pp. 198–208.
34. Kiekintveld C., Kreinovich V., Lerma O. (2011). Optimizing Trajectories for Unmanned Aerial Vehicles (UAVs) Patrolling the Border // Proceedings of the World Conference on Soft Computing, San Francisco, CA, May 23–26.
35. Kiekintveld C., Tambe M., Marecki J. (2010). Robust Bayesian Methods for Stackelberg Security Games // Conference: Autonomous Agents & Multiagent Systems/Agent Theories, Architectures, and Languages. ATAL. Pp. 1467–1468.
36. McKelvey R. D., Palfrey T. R. (1995). Quantal response equilibria for normal form games. Games and Economic Behavior. No. 2. Pp. 6–38.
37. Pate-Cornell E. (2002). Fusion of intelligence information: A Bayesian approach // Risk Anal. No. 22(3). Pp. 445–454.
38. Pita J., Jain M., Western C., Portway C., Tambe M., Ordonez F., Kraus S., Paruchuri P. (2008). Deployed ARMOR protection: The application of a game theoretic model for security at the Los Angeles International Airport. In Proc. of AAMAS.
39. Pita J., Tambe M., Kiekintveld C., Cullen S., Steigerwald E. (2011). GUARDS - Game Theoretic Security Allocation on a National Scale. In Proc. of AAMAS. Pp. 37–44.
40. Social Science for Counterterrorism. Putting the Pieces Together. Davis P.K., Cragin K. (Editors). RAND Corporation, 2009.
41. Sullivan T. J., Perry W. L. (2004). Identifying indicators of chemical, biological, radiological, and nuclear (CBRN) weapons development activity in sub-national terrorist groups // J. Oper. Res. Soc. No. 55(4). Pp. 361–374.
42. Taylor M. E., Kiekintveld C., Western C., Tambe M. (2009). 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.
43. Washburn A.R. (2010). Barrier Games // Military Operations Research. No 15(3). Pp. 31–41.
44. Wein L., Liu Y., Motskin A. (2009). Analyzing the Homeland Security of the U.S.-Mexico Border // Risk Analysis. Vol. 29. Issue 5. Pp. 699–713.
45. Wilner A. Cold War notion of deterrence works against terrorism, researcher contends // Journal of Strategic Studies: <http://www.vancouversun.com>.
46. Wright P. D., Liberatore M. J., Nydick R. L. (2006). A Survey of Operations Research Models and Applications in Homeland Security // Interfaces. Vol. 36. No. 6. Pp. 514–529.