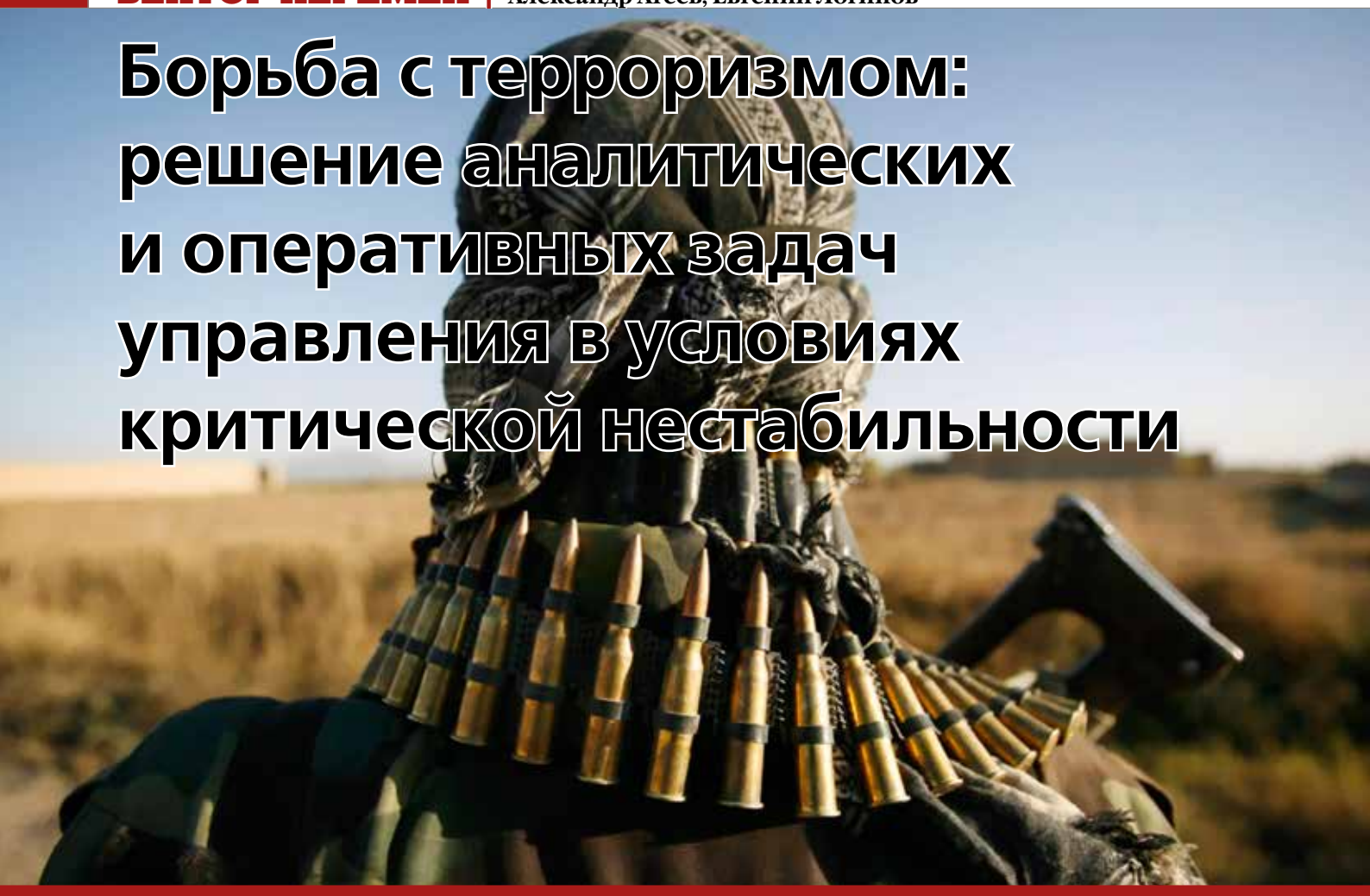
Борьба с терроризмом: решение аналитических и оперативных задач управления в условиях критической нестабильности



УДК 343.326:004.056

Серия террористических актов в Париже, падения самолетов, взрывы в разных городах мира, террористическая война против законной власти в Сирии, террор на российском Северном Кавказе – все это ставит вопрос об идущих процессах расширения террористической составляющей в практике деятельности ряда глобальных геостратегических игроков как закономерности проявления системного кризиса западной модели мироустройства. Террористические операции геостратегического характера превратились в неотъемлемый элемент глобализированной конкуренции в современной геоэкономической и геополитической среде. Необходимо осмыслить новую макротеррористическую реальность и выработать меры противостояния качественно новым рискам и угрозам безопасности нашей страны и всего мира.

Ключевые слова
Терроризм, управление, мониторинг, безопасность, инфраструктура, информационная система, анализ, прогнозирование.

Авторы

Агеев Александр Иванович — генеральный директор Института экономических стратегий ООН РАН, заведующий кафедрой управления бизнес-проектами НИЯУ «МИФИ», доктор экономических наук, профессор, академик РАЕН.
Логинов Евгений Леонидович — заместитель генерального директора Института экономических стратегий ООН РАН, заместитель директора Института проблем рынка РАН, доктор экономических наук.

Терроризм — самостоятельная военно-политическая категория, особый вид войны, компонент политической культуры и направление идейного мировоззрения, включающий силовые и иные представляющие угрозу действия, проявления и тенденции со стороны организованных структур, действующих вне формата государства.
Терроризм — это абсолютное оружие меньшинства против большинства.
Терроризм — крайняя часть спектра политического, социального, религиозного, этнического мотивированного насилия (что частично разграничивает его от организованной преступности, являющейся субъектом экономически мотивированного насилия).
Терроризм — это стратегия.
Арас Джангир [1]

Новая макро-террористическая реальность

Террористические операции геостратегического характера используются глобальными геополитическими игроками с целью изменения направлений развития различных государств, в том числе входящих в группу стран, которые, как считается, определяют судьбу мирового развития (G8, G20 и т.п.). Террористические операции геостратегического характера по своей разрушительности почти не отличаются от обычной войны, но «спрессованы» во времени и требуют от организаторов несопоставимо меньших затрат различных ресурсов, скрывая при этом заказчиков и обеляя реальных бенефициаров таких операций.

Часто за такими операциями, выполняемыми силами известных, малоизвестных и вообще никому не известных групп и отдельных лиц, явно или скрыто маячат спецслужбы различных государств [2]. По сути дела подобные операции являются грандиозными провокациями и имеют мало общего с целями деятельности религиозных или политических фанатиков, которым обычно приписывают их проведение [3].

Иначе говоря, речь идет о сверхсложной полицентрически организованной террористической мегасистеме, входящей в важнейшие (пусть и латентно) институты мирового сообщества, используемые для временного силового разрешения противоречий и фазового перехода сегмента миросистемы на основе накопившихся диспропорций к новому формату управления процессами жизнедеятельности и развития социума (они же источник накопления и мультипликации политического и финансового капитала определенных политико-экономических групп/кланов, являющихся реальными заказчиками и выгодоприобретателями таких социотеррористических кризисов) [4].

Достаточно регулярно такие операции проводятся против России.

Практически ни одно государство не может обезопасить себя от подобных рисков и угроз. События 11 сентября 2001 г. в США и серия террористических актов в Париже в середине ноября 2015 г. относятся именно к таким операциям (*рис. 1*).

Автор книги «Деньги и терроризм» Лоретта Наполеони описала этапы экономического развития терроризма следующим образом:

- во-первых, терроризм, поддерживаемый государством, который, вероятно, теряет свою значимость в межгосударственном, но не во внутригосударственном плане (нельзя не признать, что масштаб финансирования Ираном различных организаций и групп на Ближнем Востоке по-прежнему вызывает беспокойство);

Рисунок 1

Пример исследования взаимодействий террористов при планировании и осуществлении теракта 11 сентября 2001 г. в США [5]

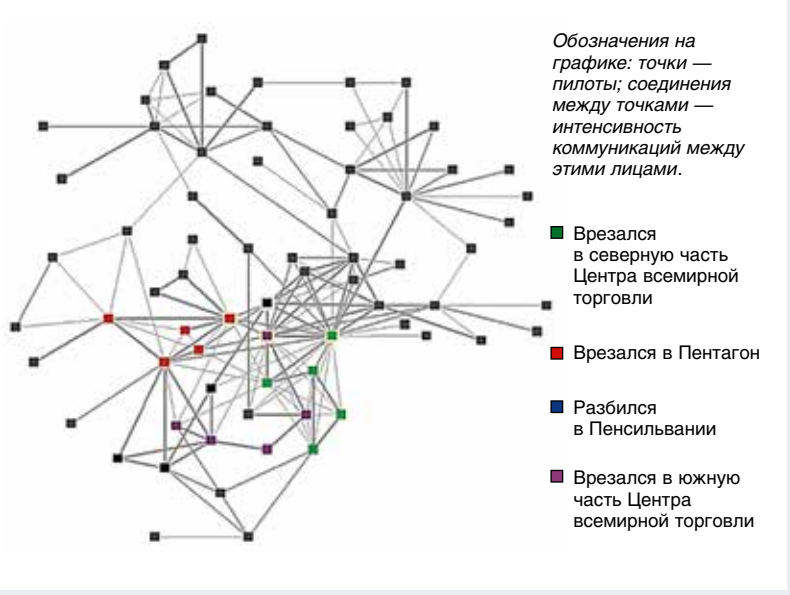
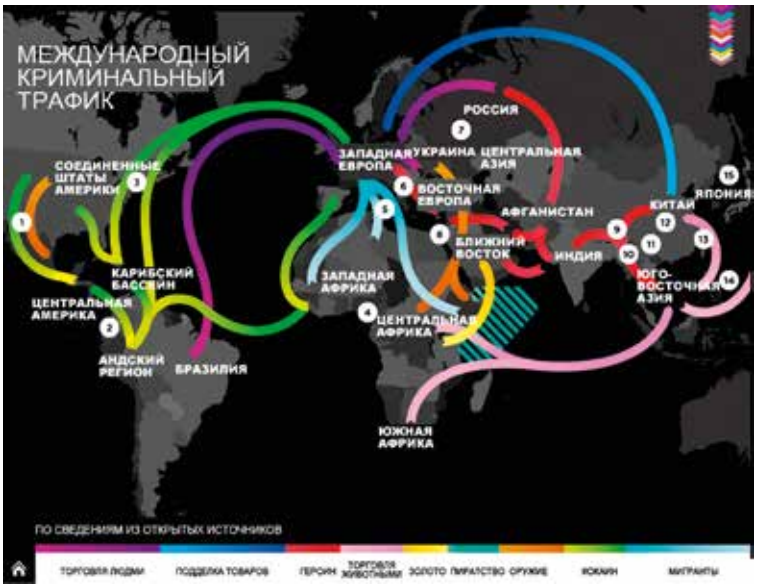


Рисунок 2

Международный криминальный трафик [6]



• во-вторых, приватизированный терроризм, когда террористические организации либо самостоятельно выбирают, либо вынуждены создавать полуавтономии в виде «государств-ракушек» (поступающие финансы и ресурсы направлены на террористическую деятельность, как, например, в Афганистане и Чечне);
• в-третьих, наивысшая форма экономической организации террористической деятельности — это глобальная террористическая сеть («Аль-Каида» и примкнувшие к ней структуры, которые извлекают выгоду из возможностей, открывающихся благодаря глобализации, ослаблению и исчезновению границ для торговли) (*рис. 2*).

Противодействие террористическим операциям геостратегического характера как мегасистеме

Противодействие террористическим операциям геостратегического характера помимо политической составляющей требует очень серьезной организационной работы, включая развитие группы базовых технологий и систем, позволяющих осуществлять мониторинг, накапливать информацию, анализировать, прогнозировать, идентифицировать угрозы, осуществлять поддержку выработки управленческих решений, планирование мер противодействия, их реализацию, сопровождение, установление обратной связи и принятие мер по совершенствованию процессов и процедур, а также развитие самих систем противодействия террористической деятельности.

В последние годы в нашей стране и за рубежом активно развиваются научно-практические разработки в области использования новых информационных технологий для противодействия различным террористическим операциям с опорой на информационные системы гражданского, военного и специального назначения.

Исходя из вышеизложенного, с учетом новой эскалации таких операций требуется совершенствование направлений и методов функционирования российского государственного механизма противодействия террористическим операциям геостратегического характера. Важнейшим элементом такого механизма является информационное обеспечение организационного процесса реализации управленческих действий на основе использования новых информационных технологий, обеспечивающих возможность практической реализации комплексного и системного подхода к решению задачи противодействия сверхсложной полицентрической организационной мегасистеме терроризма в условиях критической нестабильности.

Вообще, методы экономико-информационного обеспечения широко используются при разработке управленческих систем различного профиля. Однако при этом они рассматриваются, как правило, не в качестве элементов управленческой среды, а как технические средства выполнения некоторых производственных функций. В то же время противодействие террористическим операциям геостратегического характера предполагает выбор управленческих решений для достижения рационального компромисса между всеми принимаемыми локальными решениями в интересах избранной глобальной функциональной цели — защиты россиян и российского государства.

Поэтому, несмотря на кажущуюся аналогию традиционных задач создания управленческих систем, имеется ряд принципиальных отличий как в содержании, так и в методах их решения. Это вынуждает рассматривать задачу противодействия терроризму с учетом влияния ранее не существовавшего фактора —

террористической деятельности геостратегического характера — как существенно новую. Это диктуется также следующими причинами:

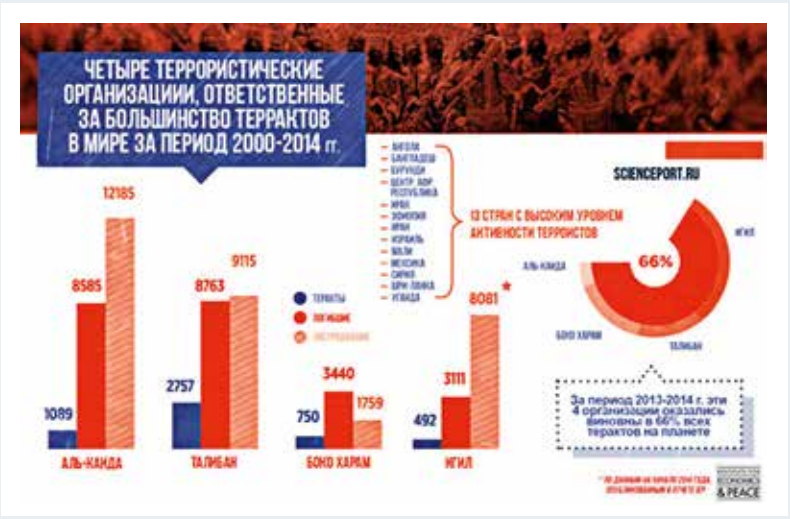
• задачи, ранее решавшиеся в процессе разработки мероприятий противодействия террористическим акциям, преследовали, как правило, локальные цели, которые выражаются в категориях априорно заданных правоохранительным органам задач и могут не соответствовать (а иногда и противоречить) целям сотрудничества различных правоохранительных ведомств. В результате это приводит к неоправданной разнотипности антитеррористических мер, их несовместимости и т.п.;

• существующие технологии противодействия террористическим акциям имеют достаточно узкую отраслевую ориентацию с применением предметно и дисциплинарно ориентированных методов, алгоритмов и средств решения правоохранительных задач, основанных, как правило, на использовании специализированных криминалистических методов и процедур. Противодействие террористической деятельности геостратегического характера как террористической мегасистеме должно осуществляться на межведомственном уровне с одновременным рассмотрением множества различных предметных областей и дисциплин. Это требует использования единого системного подхода, позволяющего синтезировать наилучшие по принятым критериальным показателям решения на межведомственном уровне;

• системное противодействие террористическим операциям геостратегического характера предполагает создание и практическое использование различных ведомственных информационных баз и банков данных, а также многоотраслевых вычислительных сетей и проблемно ориентированных новых информационных технологий, что

Рисунок 3

Динамика террористической активности [6]



не обеспечивается традиционными методами решения этих задач. Поэтому появляется необходимость в разработке специализированных методов и создании соответствующей интегрированной информационной, телекоммуникационной и вычислительной инфраструктуры;

• практическое решение задач управления страной в условиях влияния террористической деятельности геостратегического характера возможно только на основе самого широкого использования современных и перспективных информационных технологий с созданием проблемно ориентированных специализированных систем комплексной автоматизации решения правоохранительных, фискальных и контрольных задач с точки зрения совместного межведомственного противодействия террористической деятельности (*рис. 3*).

По мнению западных экспертов, в случае избрания контртеррористической стратегии прослеживается явный диссонанс между позицией администрации президента США и теми решениями, которые предлагает научное сообщество, опираясь на новейшие теоретические разработки в области изучения коммуникативно-организационных сетей. Последние достижения в области коммуникативистики становятся особенно актуальными при рассмотрении данной проблемы. Подобные разработки позволяют лучше понять природу терроризма, причины и этапы его развития, законы внутренней организации, четко определить его границы и способы противостояния ему. Неразумная контртеррористическая политика США в данном вопросе ведет к лишним, неоправданным жертвам и способствует сохранению — если не дальнейшему развитию — терроризма [7].

Трудность решения задачи повышения эффективности противодействия террористическим операциям геостратегического характера обусловлена тем, что конкретные меры, предусматривающие использование для этих целей новых информационных технологий, методов, моделей и систем, являются сугубо индивидуальными, а планирование таких мер происходит в условиях неопределенности, когда заранее часто

Сверхмощная поисковая система на основе продвинутых ботов-пауков способна вести поиск в самых отдаленных уголках Интернета, которые недостижимы для современных интернет-поисковиков.

не известны факторы и субъекты деструктивных воздействий, необходимый объем ресурсов и уровень сложности требуемых действий.

В последние годы за рубежом был реализован целый ряд проектов в этой сфере.

Ключевые программы в DARPA

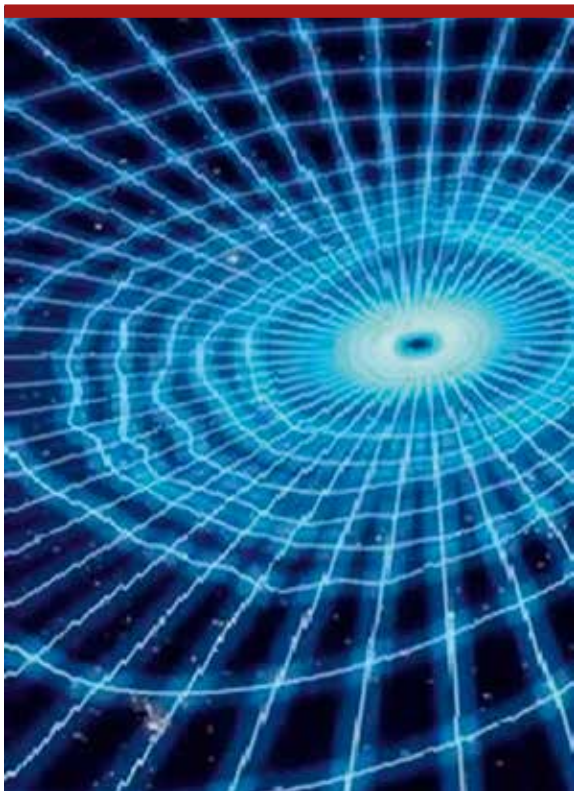
Основная цель, которую преследует DARPA (англ. *Defense Advanced Research Projects Agency* — Агентство передовых оборонных исследовательских проектов США) в проекте «Информационная осведомленность о терроризме» (*Terrorism Information Awareness*, TIA), заключается в создании системы, позволяющей на основе больших объемов несвязанной информации в различных базах данных выявить группу лиц, готовящихся совершить террористический акт на территории США: перевод с иностранных языков на английский и обратно, выявление скрытых данных и распознавание образов, корпоративный анализ информации для принятия решений.

На основе статистического анализа информации из баз данных будет определяться корреляция таких на первый взгляд случайных и не связанных между собой событий, как заказ билетов, заявки на визы, получение водительских прав, бронирование номеров в отелях, покупка химикатов и взрывчатых веществ, приобретение огнестрельного оружия и другие подозрительные действия, включая уже известные террористические акты.

В интересах эффективной обработки полученных знаний о паттернах (статистических шаблонах) поведения подозреваемых лиц будет организована совместная работа специалистов всех спецслужб, задействованных в противодействии терроризму. Используя математические методы (исследования операций, принятия решений, теории игр, вероятностные и статистические, нейросети и др.), участники корпоративных аналитических групп на основе выдвинутых гипотез о паттернах и заданных критериях целевой функции получат набор альтернатив, по которым они примут окончательное решение о проведении специальной операции по обезвреживанию подозреваемых лиц и предотвращению их предполагаемых преступных действий.

Анализ угроз внутренней безопасности США, проведенный аналитиками американских спецслужб после событий 11 сентября, показал, что в исторической ретроспективе новые вызовы оказались беспрецедентными как по масштабу, так и по асимметричности с точки зрения высокой вероятности осуществления небольшой преступной группой целой серии террористических актов с применением оружия массового уничтожения (ядерного, химического, биологического) на объектах критической инфраструктуры. Катастрофические последствия подобных терактов поставили на повестку дня задачу своевременного обнаружения таких групп и прогнозирования их возможных действий с использованием новых информационных технологий. Поэтому важное направление НИОКР в области информационных технологий для внутренней безопасности США связано с разработкой специализированного программного обеспечения так называемого ситуационного анализа (*Software for Situational Analysis*).

С этой целью DARPA выполняет ряд проектов, направленных на развитие информационных технологий, обладающих такими функциональными возможностями, как автоматическое распознавание и различение людей на расстоянии, обнаружение противника (агента), осуществляющего наблюдение за целями (объектами критической инфраструктуры) на территории США; автоматическое обнаружение, извлечение и связывание между собой отрывочных



и фрагментарных представлений о намерениях и деятельности групп людей, содержащихся в больших массивах информации из секретных и несекретных источников; достаточно точное моделирование субъективных представлений и социального поведения малочисленных по составу групп для имитации и проигрывания асимметричных действий противника; обеспечение более эффективных корпоративных средств для анализа и принятия решений в интересах повышения оперативности и эффективности распределенных групп аналитиков в динамичной обстановке.

В интересах научно обоснованного прогнозирования возможных сценариев поведения террористов при совершении преступлений DARPA разрабатывает специальный проект «Моделирование асимметричной среды» (*Wargaming the Asymmetric Environment*, WAE), который позволит аналитикам спецслужб лучше понять мотивы и разгадать замысел террористических действий. С этой целью на основе методов прикладной математики разрабатывается комплекс математических моделей, имитирующий поведение отдельных людей и небольших групп с учетом их психологии, культуры, политических взглядов, уровня образования и жизненного опыта (*Scalable Social Network Analysis*, SSNA).

Кроме того, DARPA разрабатывает имитационные модели поведения отдельных стран, их ключевых политических лидеров и террористических групп, а также аналитические модели для принятия решений, технологии отслеживания ситуаций в реальном времени (*Rapid Analytical War Gaming*, RAW). С этой целью разрабатываются специальные методы для анализа политической стабильности в регионах, прогнозирования влияния рынка стратегических технологий на состояние национальной безопасности и оценки возможных результатов перспективных программ или будущих событий (*Future Markets Applied to Prediction*, *FutureMAP*) [8].

Новые проекты DARPA, ориентированные на создание системной основы противодействия террористической деятельности, запущенные в 2015 г.

Граф-теоретические исследования эффективности алгоритмов и вычислительной архитектуры для социальных сетей

В то время как американские госведомства достигают серьезных успехов в развитии аналитических и прогнозных методов для решения задач обработки непрерывных сигналов, аналитические методы для дискретных данных, такие как графы и сети, не поспевают за ними. Последние события в мире доказывают, что анализ социальных сетей может иметь критическое значение. В данной парадигме узлы — это люди, представляющие интерес, а их отношения или взаимодействия образуют ребра графа; результат отображается в виде сети или граф. В настоящее время анализ социальных сетей находится в зачаточном состоянии, когда реальные сети представляются в грубых и примитивных элементах (диаметр, распределение узлов по числу связей и т.п.). Необходимо лучшее понимание тонкой математической структуры социальных сетей (*Graph-theoretical Research in Algorithm Performance & Hardware for Social networks*, GRAPHS).

Технологии вероятностного программирования для самообучающихся машин

Программа PPAML ставит целью построить машины, которые

будут учиться с помощью алгоритмов вероятностного программирования просеивать огромные базы данных и выбирать наилучшие варианты решения проблемы. В ходе этой работы искусственный интеллект будет учиться и, спустя некоторое время, сможет легко решать простые задачи. Технология PPAML поможет более эффективно решать множество аналитических задач, которые сегодня требуют огромных людских ресурсов, — таких как разведка, наблюдение, распознавание речи, вождение автомобиля, просеивание информации в поисках ценных данных и т.д. При этом аппаратное обеспечение может быть разнообразным — суперкомпьютеры на базе многоядерных процессоров, кластеры обычных ПК и облачные сети (*Probabilistic Programming for Advancing Machine Learning*, PPAML).

Транспаретные вычисления

В рамках программы «Транспарентные вычисления» разрабатываются технологии, позволяющие осуществлять более эффективную политику безопасности в распределенных системах. Масштаб и сложность современных информационных систем скрывают связи между событиями, сопряженными с безопасностью, в результате чего работа по обнаружению атак и аномалий приходится на специализированную контекстную информацию, а не на доскональное знание происхождения события. Этот недостаток позволяет выполнять такие атаки, как подмена (на уровне пользователя) и мимикрия (на уровне машинного кода). Программа ставит целью разработку нескольких перспективных подходов к этим проблемам. Результаты программы особенно важны для крупных интегрированных систем с разнородными компонентами, таких как распределенные системы видеонаблюдения, автономные системы и корпоративные информационные системы (*Transparent Computing*).

ADAMS

Программа ADAMS разрабатывает приложения, предназначенные для выявления аномальных процессов, происходящих в обществе, наблюдения за неадекватным поведением отдельных индивидуумов и групп людей (*Anomaly Detection at Multiple Scales*).

Глубокий анализ и фильтрация текстовых материалов

Программа разработана для помощи военнослужащим, работа которых связана с принятием решений на основе выводов, полученных из скрытой в текстах информации, фильтрующей избыточные и соединяющей подобные документы. Значительная часть оперативной информации может быть выражена скорее в имплицитном, нежели в эксплицитном виде; в большинстве случаев информация намеренно запутана, а важные действия и объекты представлены исключительно непрямым образом. Создаваемые в рамках DEFT технологии автоматизированного глубокого понимания естественного языка смогут обеспечить разработку усовершенствованного решения для более эффективной обработки текстовой информации, исключая возможность двусмысленного понимания со стороны человека-оператора (*Deep Exploration and Filtering of Text*, DEFT).

Высокая чувствительность к иностранным языкам

Программа FLRR предусматривает разработку методов быстрого конструирования переводческих технологий для произвольных иностранных языков. Исторически сложилось так, что использование материалов на иностранном языке требует продолжительных усилий; в результате системы автоматизированного перевода существуют только для наиболее распространенных языков. Вооруженные силы действуют глобально и часто сталкиваются с редкими языками, для которых нет никаких автоматизированных переводческих технологий. Технологии FLRR идентифицируют общности между недавно обнаруженным редким языком и распространенными языками и идентифицируют языковые универсалии для быстрой переориентации существующих переводческих технологий на редкий язык. Это позволит быстро создавать системы автоматизированного перевода для кроссязыковой разведки и стратегических коммуникаций (*Foreign Language Rapid Response*, FLRR).

В рамках сетецентрической информационной решетки антитеррористической (в том числе антикриминальной) деятельности возможно выявить ключевых субъектов, даже если точная структура организационной сети неизвестна.

XData

Программа XData разрабатывает вычислительные методы и программные инструменты анализа больших объемов данных как «полуструктурированных», так и неструктурированных. Планируется решить следующие основные задачи: создать масштабируемые алгоритмы обработки «сырых» данных в распределенных хранилищах; создать эффективные средства взаимодействия человека с компьютером, позволяющие с помощью настраиваемых визуализаций делать логические выводы из данных, полученных в ходе всевозможных миссий. В рамках программы будет поддержано развитие инструментариев с открытым кодом, чтобы оперативно создавать программное обеспечение для обработки больших объемов данных в сроки, заданные требованиями оборонных проектов (XData).

Система автоматизированного контент-анализа изображений и мультимедиа

Сегодня объем визуальных данных необычайно быстро растет; уже сейчас с точки зрения возможностей контент-анализ опережает ручной анализ, не говоря уже о том, чтобы анализировать каждое изображение в отдельности. В рамках программы VMR будет разработано программное обеспечение, позволяющее визуально исследовать миллионы цифровых фотографий и каталогизировать их по тому или иному признаку (*Visual Media Reasoning*, VMR).

Memex

Программа *Memex* разрабатывает информационные технологии, способные быстро и тщательно организовать подмножество сведений из Интернета. В рамках работы программы будут рассмотрены недостатки централизованного поиска для предметно ориентированной индексации вебконтента, а новый алгоритм поиска обеспечит быстрый, гибкий и эффективный доступ к предметно ориентированному содержанию. В результате реализации программы сверхмощная поисковая система на основе продвинутых ботов-пауков будет способна вести поиск в самых отдаленных уголках Интернета, которые недостижимы для современных интернет-поисковиков, обеспечивая своим пользователям технологическое превосходство в области индексации контента и вебпоиска (*рис. 4*).

WISR

Система сбора информации, наблюдения и разведки по всему миру (WISR) обеспечит работоспособность систем ISR в за-

Рисунок 4

Визуализация, показывающая лишь часть наших коммуникационных сетевых маршрутов [9]

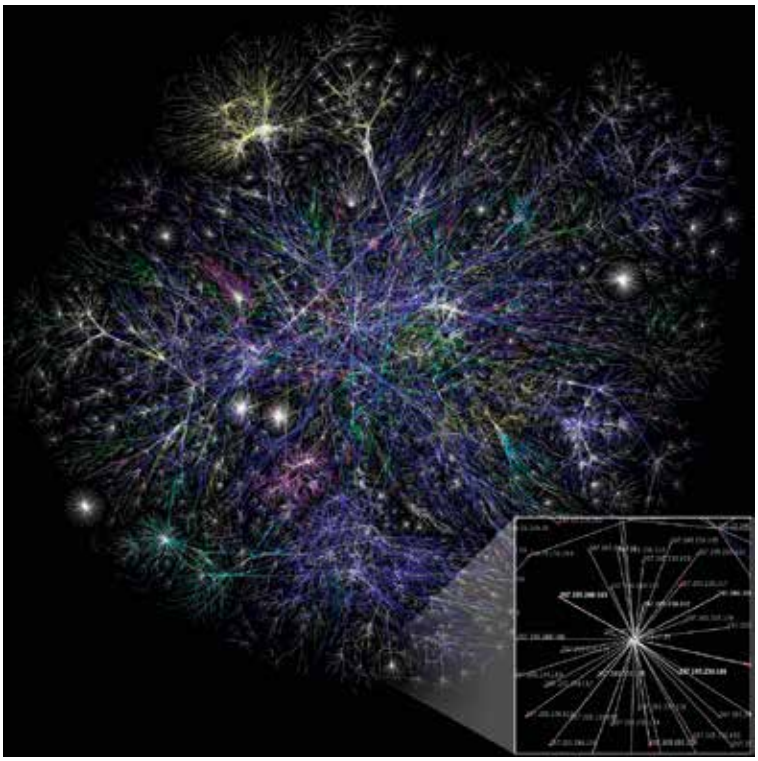
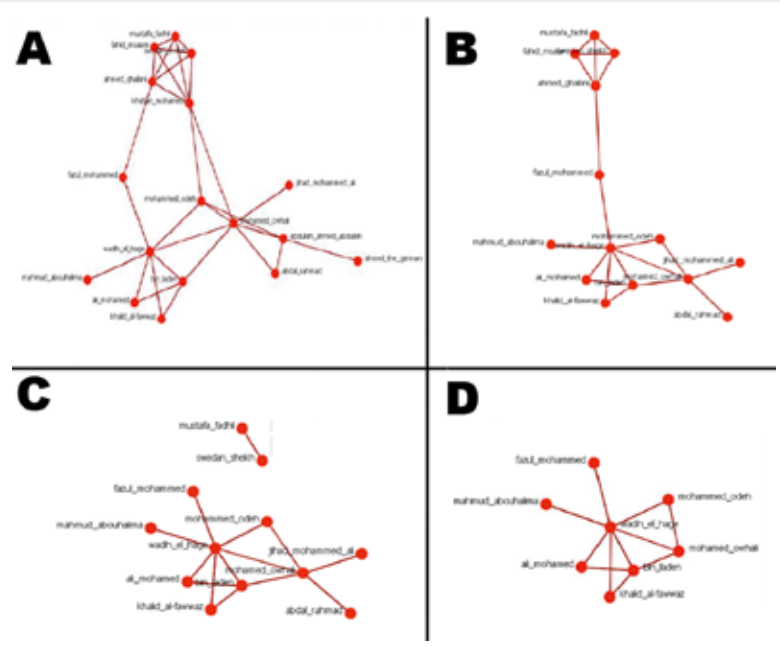


Рисунок 5

Схема вычисления ключевых узлов в террористической сети: удаление ключевых узлов террористической сети делает ее более хрупкой [11]



претных зонах. Американские войска ограничены в использовании бортовых систем разведки, наблюдения и рекогносцировки (ISR) во многих критически значимых проблемных областях. В то же время миллионы отправляемых по всему миру видеороликов, число которых быстро увеличивается, отражают интересные для национальной безопасности события. В рамках программы WISR будет произведена интеграция видео и изображений в 3D- и 4D-реконструкции событий, позволяющая отслеживать динамические изменения. Методы WISR также могут быть использованы для отслеживания культурных и социальных изменений при подготовке к вводу на территорию экспедиционных войск (*Worldwide Intelligence Surveillance and Reconnaissance*, WISR).

Доказательства агрессии

Сегодня основной объем работы по судебно-криминалистической экспертизе приходится на аналитиков и следователей, кропотливо собирающих всю доступную информацию и представляющих полученные данные в виде логической цепочки событий. Программа предусматривает создание технологий для поиска и сопоставления разнообразных типов неструктурированной информации, включая медиаматериалы, с целью получения необходимых доказательств, обличающих злоумышленников. Планируется развить, объединить и расширить технологии поиска по тексту, речи и видеоинформации, что позволит представлять соответствующую пространственно-временную информацию. Программа также разовьет и применит методы, позволяющие аналитикам эффективно, в том числе и на уровне интуиции, выявлять подозрительные действия, неочевидные отношения и другие зацепки для проведения последующих оперативных мероприятий (*Battlefield Evidence*) [10].

Другие зарубежные информационно-аналитические технологии антитеррористического (антикриминального) характера

Ученые из *Network Science Center* Военной академии Вест-Пойнт (США) разработали алгоритм, который позволяет вычислять ключевые узлы в террористической сети и разрушать ее (*рис. 5*).

Алгоритм GREEDY_FRAGILE не просто выполняет банальную задачу обнаружения «медийных» террористов, которые постоянно на слуху, но зачастую к реальной вооруженной борьбе имеют косвенное отношение. Разработка американских военных ученых направлена на разрушение террористической сети. Например, алгоритм может выявить террористов-командиров среднего уровня, которые командуют боевыми группами. Если этих командиров устранить, командование террористической сетью вынужденно концентрируется в руках одного-двух человек, убив которых, можно разрушить или парализовать деятельность всего террористического подполья. Таким образом, полагается, что вместо уничтожения лидера нужно, наоборот, делать террористическую сеть более централизованной. Такая сеть из-за концентрации властных полномочий станет более хрупкой и впоследствии, после уничтожения лидера, рассыплется на отдельные менее опасные группки и террористов-одиночек.

Теперь с разработкой GREEDY_FRAGILE появилась возможность выявить ключевых террористов, даже если точная структура террористической сети неизвестна, а использование внедренных агентов или других разведсредств невозможно.

В ходе испытаний нового алгоритма использовались хорошо изученные данные по пяти террористическим сетям, в частности по подразделению «Аль-Каиды», которое участвовало в подрыве посольства США в Дар-эс-Саламе в 1998 г.

GREEDY_FRAGILE показал, что в каждой из пяти реальных террористических сетей удаление только 12% узлов может увеличить централизацию всей сети на 17–45%. Таким образом, постепенно удаляя ключевые фигуры, можно делать террористическую организацию все более хрупкой и беспомощной [11].

Еще один аналогичный проект. Группа ученых из Италии и США при помощи сетевого анализа описала основные структурные характеристики сицилийской мафии, а также проанализировала, как будет меняться сеть контактов гангстеров в различных сценариях полицейских операций.

Авторы разработки использовали архив данных полиции Северной Сицилии, куда входили следственные данные по делам мафии, а также материалы, полученные в ходе слежки, записи телефонных разговоров и пр. На основании этой информации ученые построили два графа, которые и анализировались в ходе работы (*рис. 6, 7*).

Первый граф представлял собой сеть контактов, в которой каждой вершине соответствовал один подозреваемый; вершины считались связанными, если между ними был совершен хотя бы один телефонный звонок. Второй граф авторы назвали сетью преступлений; в него входили все члены мафии, которым были предъявлены непосредственные обвинения. При этом две вершины были связаны, если оба преступника проходили по одному делу или заявляли, что видели друг друга на месте преступления.

Рисунок 6

Графы контактов мафии Северной Сицилии [12]

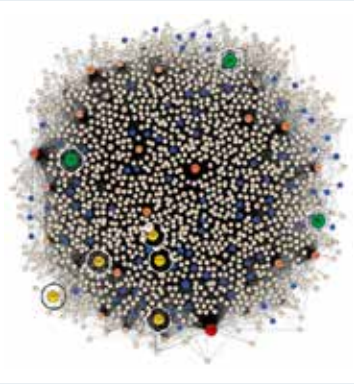
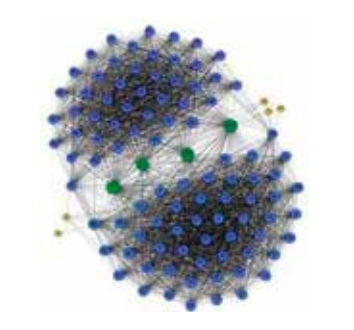


Рисунок 7

Графы преступлений мафии Северной Сицилии [12]



На основании сведений полиции ученые нанесли на графы предполагаемую «должность» каждого мафиози, чтобы выяснить, как отличается вовлеченность в сеть контактов в зависимости от места в иерархии. Оказалось, что боссы мафии имели минимальное число контактов с остальными членами группировки, поддерживая связь через «лейтенантов».

Кроме того, результаты кластерного анализа показали, что существует большое число «посредников». По мнению авторов разработки, этот класс организует контакты между сторонними лицами и тесно связанными группами внутри семьи.

Также ученые проследили, как изменяется структура графов,

если из них удалить определенную долю вершин. Эта модель соответствует действиям полиции, в результате которых изолируется какое-то количество членов мафии. В случае если вершины удалялись из графа одновременно, сеть контактов резко теряла связность, тогда как сеть преступлений практически не претерпевала изменений в структуре. В случае когда вершины устранялись последовательно, а не одновременно, структура обоих сетей оказывалась более стабильной [12].

Есть в этой сфере и эффективные российские технологии. Среди таких технологий, о которых имеются публикации в открытом доступе, можно выделить следующие.

Российские информационно-аналитические технологии антитеррористического (антикриминального) характера

В Институте прикладной математики имени М.В. Келдыша разработан математический алгоритм, позволяющий прогнозировать изменение уровня преступности. Прогноз делается на основе гипотезы о том, что количество преступлений представляет собой наблюдаемую величину, характеризующую некую сложную, иерархически организованную систему, охватывающую общество в целом. Прогноз делается на основе данных о динамике преступности в предшествующий период времени. Предложенный авторами работы подход аналогичен используемому при прогнозировании землетрясений (закон Гутенберга — Рихтера). В настоящее время достигнут уровень предсказания всплесков числа преступлений, соответствующий 70 процентам, притом что продолжительность «тревожных периодов» составляет около 30 процентов [13].

Технология создания простых и удобных 4D-ГИС стала доступной с появлением в последней версии клиентской программы популярного сервиса *Google Earth* поддержки отображения изменения объектов во времени — функции тайм-слайдер. На базе системы учета географии преступности, созданной группой ГИС Института физики высоких энергий, продемонстрированы возможности мониторинга событий и в пространстве, и во времени. С помощью тайм-слайдера становится возможным оперативно и без усилий для пользователя в 3D-режиме отслеживать динамику развития преступности. Мгновенно проявляются особенности, выявить которые при представлении информации в табличном виде либо в виде ГИС чрезвычайно трудно — концентрация событий в локальных областях, события «серийного» характера и многое другое.

США продолжают наращивать качественный отрыв от других стран, включая Россию, по информационно-аналитическим технологиям, используемым спецслужбами.

Несмотря на активно ведущиеся разработки в этой сфере, наблюдается определенное отставание идей по проблеме контртеррористической и подобной ей деятельности в отношении качественно новых объектов организационной среды, свойственных либеральной рыночной экономике (например, неформализованные явно или латентно деструктивные сетевые сообщества, трудно локализуемые «блуждающие» очаги антигосударственной или иной незаконной деятельности и пр.). Появляется специфический вид инициированной потери управляемости на основе латентных организационных сетей террористического или просто криминального характера, пока не отраженный как в научных исследованиях, так и в практических разработках соответствующих госорганов и служб.

Традиционные модели террористических, диверсионных и иных ситуаций здесь часто нельзя взять за основу, поскольку средства и способы деструктивного воздействия могут оказаться принципиально новыми: вследствие применения как принципиально новых технологий террористической деятельности, так и методов действий террористов и их пособников, которые в ряде случаев могут находиться за пределами сферы их возможного упреждающего обнаружения и идентификации.

Интересным решением проблем мониторинга, идентификации и прогнозирования террористических операций геостратегического характера является российская разработка по созданию информационно-аналитического комплекса мониторинга электронных сообщений в глобальных телекоммуникационных сетях. Данный комплекс строится на основе мониторинга информации в открытом доступе (адресно-временного трафика электронных трансакций): анализируется внешняя динамика генерации определенными лицами информационных сообщений во временной и адресной разбивке для выяснения устойчивых связей с определенными структурами, что полностью соответствует нынешнему российскому законодательству, а также не противоречит курсу российского государства на соблюдение демократических принци-

пов и продолжение рыночных реформ (*рис. 8*).

Реализована разработка электронной нейромодели для обеспечения выявления устойчивых связей между субъектами рынка и причинно-следственных связей между деятельностью субъектов рынка, с одной стороны, и событиями и процессами в экономике и общественной жизни, с другой стороны, в процессе проведения мониторинга и анализа трафика электронных трансакций в глобальных телекоммуникационных сетях.

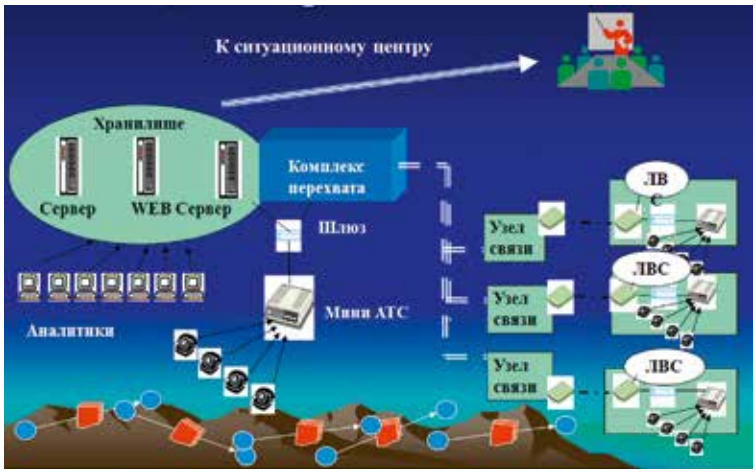
Данный комплекс создан на основе математического аппарата потоковых графов и нейромоделирования, которые были ранее разработаны в рамках работы по кластеризации движущихся объектов, обладающих комплексом разнородных характеристик в условиях высокого уровня стохастических шумов и помех искусственного происхождения.

Нейросетевое моделирование с использованием информации, полученной путем анализа трафика электронных трансакций, позволяет прогнозировать деятельность экономических структур на качественно новом уровне, что дает возможность получить итоговую резюмирующую информацию об объекте, отсутствующую в явном виде в информационных источниках.

Конкретными направлениями практического применения представленного комплекса являются:
• использование для фискального мониторинга, оперативно-розыскных мероприятий правоохранительными органами и спецслужбами России;
• использование для макроэкономического анализа, прогнозирования экономического развития и экономической конъюнктуры государственными министерствами и ведомствами;

Рисунок 8

Схема информационно-аналитического комплекса мониторинга электронных сообщений в глобальных телекоммуникационных сетях [14]



• использование для политического анализа политическими партиями, общественными и научно-исследовательскими организациями.

Ключевые характеристики информационно-аналитических систем антитеррористического (антикриминального) назначения

Такие системы должны позволять делать следующее.

Анализ связей. Метод позволяет выявить явные и неявные (скрытые) отношения и цепочки связей между различными объектами — лицами, организациями, событиями и т.д. Аналитические диаграммы связей представляют эту информацию в наиболее наглядном и понятном виде, что существенно помогает в подготовке выводов.

Анализ потоков. Данный метод является важным расширением анализа связей, так как суть преступной деятельности и ее организации может быть раскрыта через анализ перемещения предметов, имеющих отношение к этой деятельности. Анализ потоков позволит представить механизм преступления наиболее наглядно и таким образом поможет в подготовке вывода.

Временной анализ событий. Метод позволяет более четко представить развитие сложных ситуаций во времени: установить последовательность событий, их хронологию, характер связи между событиями и роли основных участников.

Анализ бизнес-процессов (процесса деятельности, в том числе преступной). Метод используется для визуализации последовательности действий, направленных на достижение конкретной цели. Построенные схемы отражают принцип деятельности и устанавливают типичный способ совершения преступления. Метод может эффективно использоваться, в частности, в целях противодействия преступной деятельности.

Табличный и кросс-табличный анализ. Традиционный метод табличного анализа необходим для проверки и предварительной оценки данных (методы

сортировки, фильтрации и т.д.); используется для выделения значимой информации в целях дальнейшего детального исследования. Кросс-табличный анализ в комплексе с методами визуализации детальных данных позволяет наиболее эффективно вести анализ статистики и готовить сложные отчеты для стратегического уровня управления.

Картографический анализ. Знание времени и места преступления/происшествия порой жизненно необходимо для принятия оперативных мер. Картографический анализ (маршруты, расстояния, геокоординаты объектов, пространственно-временной анализ событий, очаги преступной активности, тематические карты и т.д.) позволяет принимать решения на основе более точной и своевременной информации.

Графика. Методы образного представления информации широко используются для осуществления оперативного анализа многомерных данных (OLAP) и формирования отчетности [15].

В результате у антитеррористического правоохранительного сообщества появятся возможности:
- выявлять скрытые отношения — обнаруживать связи между преступными организациями и их членами;
- вскрывать организационную структуру преступных сообществ — устанавливать и фиксировать иерархические отношения между членами преступных организаций;
- устанавливать подпольную инфраструктуру преступных сообществ — обнаруживать связи с другими организациями и отдельными лицами, выявлять местоположение, оборудование и сети связи;
- выявлять финансовые операции преступных сообществ — вскрывать источники и каналы финансирования для совершения преступлений;
- выявлять типичные признаки подозрительного поведения — устанавливать и анализировать признаки подозрительного поведения членов «групп риска» с целью своевременного обнаружения возникающих угроз;
- вскрывать уязвимые места — выявлять источники финансирования и материального обеспечения преступной деятельности, склады и другие ресурсы преступных групп и сообществ, способы связи между отдельными преступниками и организованными группами, а также методы вербовки их участников с целью обнаружения особенностей, которые могут быть использованы для предупреждения, пресечения и расследования преступлений [16].

Опыт США показывает, что именно информационно-аналитические технологии создают качественно новую, ранее недостижимую прозрачность поля финансовых и других операций юридических и физических лиц. США продолжают наращивать качественный отрыв от других стран, включая Россию, по информационно-аналитическим технологиям, используемым спецслужбами. В США создана мощная группировка разведывательных, коммуникационных и вычислительных систем, создающих качественно новые возможности анализа практически любого оперативного пространства, в том числе предусматривающие моделирование и вскрытие латентных отношений между внешне не связанными динамичными системами, отражающими любые интересующие американского аналитика характеристики.

С учетом этого опыта необходимо повышение эффективности российских антитеррористических механизмов за счет интеграции в единый комплекс оргструктур и информационных систем различных государственных ведомств, что наиболее эффективно может быть формализовано как сетецентрическая информационная решет-

ка антитеррористической (в том числе антикриминальной) деятельности государственных органов.

Сетецентрическая информационная решетка антитеррористической деятельности

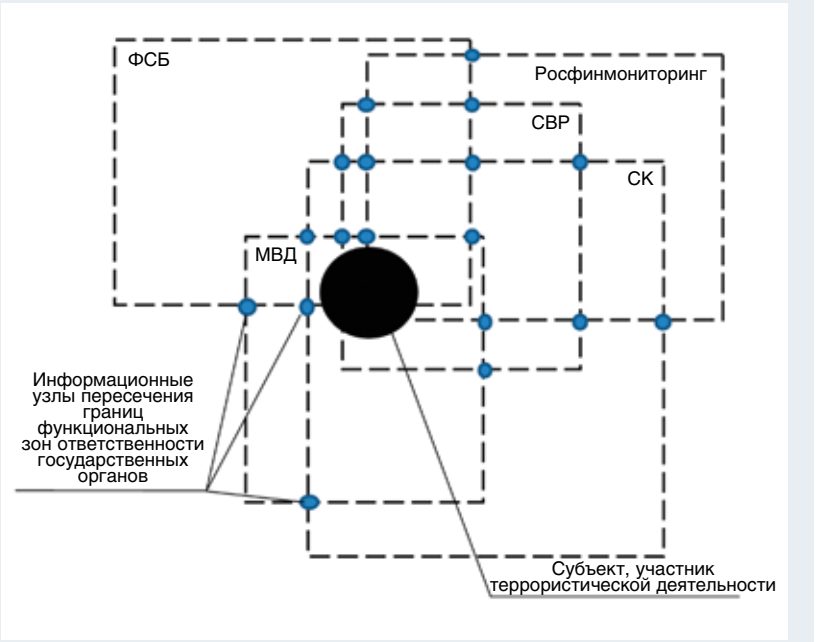
Сетецентрическая информационная решетка антитеррористической (в том числе антикриминальной) деятельности государственных органов позволяет обеспечить новое качество антитеррористического управления — организационной структуризации процессов и процедур антитеррористической (в том числе антикриминальной) деятельности государственных ведомств всех уровней. Сетецентрическая информационная решетка расширяет управленческую модель мониторинга и координации за пределы одного ведомства, сетецентрически интегрируя взаимоотношения по информационно-технологическим цепочкам сбора, обработки, хранения и обмена информаций (на основе больших объемов несвязанной информации в различных базах данных) в рамках кластера органов государственного управления, контролирующих и правоохранительных органов.

В рамках сетецентрической информационной решетки антитеррористической (в том числе антикриминальной) деятельности возможно выявить ключевых субъектов, даже если точная структура организационной сети неизвестна, а также осуществить позиционирование выявленного субъекта как объекта антитеррористической (в том числе антикриминальной) деятельности государственных органов (*рис. 9*).

Данный подход предъявляет особые требования ко всем этапам стратегического обеспечения взаимодействия всей совокупности государственных ведомств, принимающих участие в антитеррористической деятельности на основе выявления информационных связей между узлами пересечения границ функциональных зон ответственности государственных органов в рамках сетецентрической информационной решетки антитеррористической (в том числе антикриминальной) деятельности (*рис. 10*).

Рисунок 9

Позиционирование субъекта как объекта антитеррористической деятельности государственных органов в рамках сетецентрической информационной решетки антитеррористической деятельности [17]



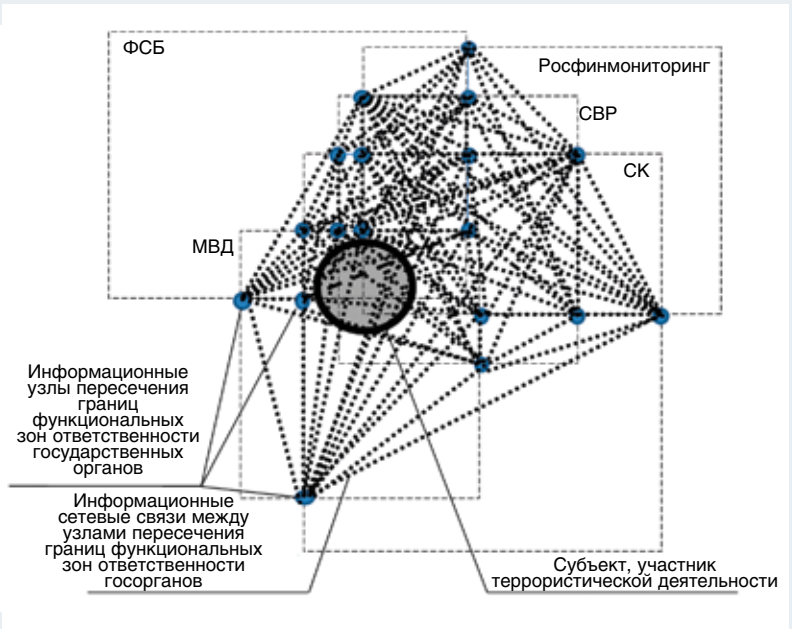
В рамках выявленных информационных связей производится структуризация функциональной деятельности различных органов государственного управления, контролирующих и правоохранительных органов. Это обеспечивает быстроту реагирования на изменяющуюся ситуацию за счет принятия своевременных обоснованных решений и ускоренного доведения их до структурных подразделений государственных органов. Причем планирование таких мер происходит в условиях неопределенности, когда заранее не известны факторы и субъекты деструктивных воздействий, необходимый объем ресурсов и уровень сложности требуемых действий.

Комплекс функциональных трансакций удобно изложить в рамках матрицы антитеррористических действий государственных органов в отношении идентифицированного субъекта (*рис. 11*).

Такой комплекс мониторинга обеспечивает итоговый выход кластера органов государственного управления, контролирующих и правоохранительных органов на новое качество управления на основе ситуационной осведомленности путем формирования целостной многоуровневой системы управления с увеличением объемов получаемой и анализируемой информации и повышением критической надежности всей системы, включая самые слабые и уязвимые звенья, в том числе за счет

Рисунок 10

Информационные связи между узлами пересечения границ функциональных зон ответственности антитеррористической деятельности государственных органов в рамках сетецентрической информационной решетки антитеррористической деятельности [18]



изменения подходов к оценке исходных факторов и принятия управленческих решений в сфере мониторинга, идентификации и предотвращения террористических операций.

* * *

Новые разработки в этой сфере направлены на обеспечение внедрения более устойчивых вычислительных и коммуникационных технологий и создание совершенно новых подходов к обеспечению использования информационных сетей и вычислительных систем. Эти технологии создают качественно новые возможности в сфере мониторинга, идентификации и прогнозирования террористических операций геостратегического характера; гарантируют более эффективное использование сетевых ресурсов и повышение производительности вычислительной и коммуникационной инфраструктуры. Применение новых информационных систем в этой сфере должно обеспечить лучшее понимание окружающей природной, технологической и социальной среды, возможностей, намерений и действий союзников и противников, расширение прав и возможностей участников процесса управления, формирование эффективной стратегии, тактики и планов, осуществление оперативного управления людьми и ресурсами, необходимого для достижения успеха в этой сфере деятельности. ЭС

ПЭС 15157/01.12.2015

Источники

1. Джангир А. О четвертой мировой войне [Электронный ресурс] // Русский архипелаг. 2003. URL: http://www.archipelag.ru/geopolitics/piryadok/terror/fourth/

2. Холодная война — 2.0: реалии и перспективы // Экономические стратегии. 2015. № 2. С. 74–79.

3. Агеев А.И. Силовая экономика и смена мирового гегемона // Стратегические приоритеты. 2015. № 2. С. 27–48.

4. Логинов Е.Л. Глобализационная парадигма терроризма: Терроризм как стратегический инструмент глобализированной конкуренции // Системные проблемы экономической безопасности: Собр. соч. в 20 т. М.: Научтехлитиздат, 2008. Т. 17. 296 с.

5. Прохоров А., Ларичев Н. Компьютерная визуализация социальных сетей [Электронный ресурс] // КомьютерПресс. 2006. URL: http://compress.ru/article.aspx?id=16593iid=771.

6. Международный криминальный трафик [Электронный ресурс] // ТерроруНЕТ. URL: http://www.terrorunet.ru/infographics/?SHOWALL_1=1.

7. Stohl, C., Stohl, M. Networks of Terror: Theoretical Assumptions and Pragmatic Consequences // Communication Theory. 17 (2007). P. 93–124.

8. В интересах национальной безопасности [Электронный ресурс] // Agentura.ru. URL: http://www.agentura.ru/dossier/usa/darpa/

9. Хижняк Х. Что произойдет, если человечество лишится всех искусственных спутников? // http://hi-news.ru/technology/chto-proizojdet-esli-chelovechestvo-lishitsya-vsex-iskusstvennyx-sputnikov.html.

10. Исследовательская программа DARPA на 2015 год [Электронный ресурс] // МФТИ. 2014. URL: https://mipt.ru/education/chairs/theor_cybernetics/government/upload/3af/Program_darpa2015_rus.pdf.

11. Callahan, D., Shakarian, P., Nielsen, J., Johnson, A. Shaping Operations to Attack Robust Terror Networks [Электронный ресурс] // Cornell University Library. URL: http://arxiv.org/pdf/1211.0709.pdf.

12. Agreste, S., Catanese, S., De Meo, P., Ferrara, E., Fiumara, G. Network Structure and Resilience of Mafia Syndicates [Электронный ресурс] // Cornell University Library. URL: http://arxiv.org/abs/1509.01608.

13. Кузнецов И.В., Родкин М.В., Серебряков Д.В. Прогноз скачков тяжких преступлений на основе иерархичности режима преступности [Электронный ресурс] // ИПМ

им. М.В. Келдыша РАН. URL: http://www.keldysh.ru/papers/2005/prep12/prep2005_12.html.

14. Создание информационно-аналитического комплекса мониторинга электронных сообщений в глобальных телекоммуникационных сетях / А.С. Бугаев, В.Н. Сараев, В.К. Лаев, Е.Л. Логинов, В.А. Мищенко, А.Н. Райков, А.В. Руднев, И.В. Шевченко, Н.Д. Эриашвили. М., 2006.

15. Аналитический комплекс Security AS (Security Analyst's Station) [Электронный ресурс] // iRule. ULH: http://irule.ru/reshenija/universalnoe-reshenie-security-as.html.

16. Правоохранительные органы России осваивают четвертое измерение // http://rnd.cnews.ru/news/top/index_science.shtml?2006/12/11/229331.

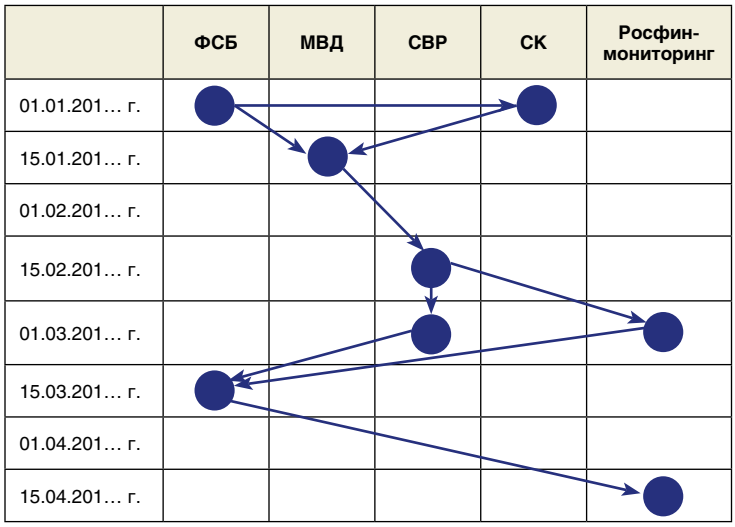
17. Логинов Е.Л., Матвеев А.Г. Информационно-коммуникационные приоритеты обеспечения эффективности антикриминальных действий государственных ведомств в экономике России // Экономические науки. 2010. № 70. С. 17–21.

18. Логинов Е.Л., Матвеев А.Г Повышение эффективности управленческой деятельности государственных органов в экономике России на основе сетецентрической информационной решетки антитеневой деятельности // Экономические науки. 2010. № 70. С. 32–36.

19. Логинов Е.Л., Матвеев А.Г. Проблемы выявления и идентификации участников организационных сетей, осуществляющих скрытое оперирование финансовыми и имущественными активами // Борьба с коррупцией как ключевой элемент усиления мировой системы ПОД/ФТ: Материалы международной научно-практической конференции. Москва, 14 мая 2015 г. // Федеральная служба по финансовому мониторингу, Международный учебно-методический центр финансового мониторинга; под. ред. В.И. Глотова. М.: МУМЦФМ; Ярославль: Литера, 2015. С. 44–50.

Рисунок 11

Матрица антитеррористических действий государственных органов в отношении субъекта [19]



The Struggle Against Terrorism: Control Problems Solution Under Critical Instability Conditions

Alexander Ageev, Evgeny Loginov

A series of terrorist attacks in Paris, plane crashes, explosions in different cities around the world, a terrorist war against the legitimate government in Syria, the terror in Russia's North Caucasus — all these phenomena called forth the problem of ongoing processes of the terrorist component expansion in the global geo-strategic players' activities like regularity pattern manifesting the systemic crisis of the western world order model. Geostrategic nature of terrorist operations is an integral part of the globalized competition in contemporary geo-economic and geopolitical environment. It is necessary to comprehend the new macro-terroristic reality and to develop measures to confront qualitatively new risks and threats to our country's security and whole world's.

Keywords: terrorism, management, monitoring, security, infrastructure, information system, analysis, forecasting.