УДК 004.891, 004.942

В.М. Шишкин

МОДЕЛИ КОМПЛЕКСНОЙ ОЦЕНКИ ФАКТОРОВ РИСКА И ДИНАМИКИ УГРОЗ ТЕРРОРИСТИЧЕСКОЙ НАПРАВЛЕННОСТИ

Технологии ведения террористической деятельности имеют комплексный характер и, следовательно, противодействие угрозам соответствующей направленности нельзя рассматривать исключительно как выявление и предотвращение инцидентов, т. е. в контексте оперативной работы, – результативность такого подхода будет заведомо ограниченной.

Отдельно следует остановиться на информационно-психологических воздействиях. Террористические цели предполагают то или иное влияние на психику, моральное состояние как масс, так и лица, принимающего решения, чтобы были получены материальные или политические результаты.

Понятно, что используются не только узкоспециальные методы и средства, но и широкий спектр разнообразных воздействий на психологическое состояние как на индивидуальном, так и групповом уровне. Наряду с собственно психологическими методами и средствами применяются трудно определяемые и неизмеряемые, но объективно существующие и крайне важные для безопасности, выражаемые на ментальном, интеллектуальном, культурном, аксиологическом, духовном уровнях. Нельзя в этот ряд не включить и так называемый человеческий фактор – комплекс угроз безопасности в человеко-машинных, социотехнических системах, которые связаны с разнообразными проявлениями поведенческих особенностей людей во взаимодействии с технологической средой. Если абстрагироваться от деталей, то все риски нарушения безопасности имеют системный техно-гуманитарный характер.

Таким образом, в первую очередь при рассмотрении процессов противодействия террористическим угрозам следует обратить внимание на сложность и неопределенность системы взаимодействий разнородных факторов с многочисленными обратными связями, что в результате может дать неожиданные эффекты в любой сфере, материальной и нематериальной, независимо от собственно террористических целей. Поэтому для исследования данной проблематики необходим адекватный ее сложности методический аппарат и инструментарий, способный учесть неопределенность и разнородность исходной информации при определении обоснованных метрически сравнимых оценок всему спек-

тру угроз. Только тогда, имея оценку значимости угроз, можно будет целенаправленно и эффективно противодействовать им, причем не исключено, что решение проблем противодействия террору придется искать в далеких от него сферах.

При этом следует также учитывать двойственный характер любых мер противодействия угрозам: их применение способно одновременно с желаемым результатом по отношению к одним факторам вызвать негативные последствия относительно других. Примером необходимости учета данного обстоятельства в антитеррористических мероприятиях может служить катастрофа самолета German wings в начале 2015 г., когда именно антитеррористическая защита создала условия для действий пилота, по сути, террористических. Другим примером, весьма актуальным сегодня, является широкое информирование о совершенных терактах, проведении публичных антитеррористических мероприятий. С одной стороны, оно мобилизует общество и создает некоторые препятствия повторению терактов, но с другой, опять-таки учитывая психологические особенности разных людей и групповое поведение, особенно в мегаполисах, во-первых, создает атмосферу страха, тревоги, что и является одной из целей теракта, а во-вторых, стимулирует людей с неустойчивой психикой на совершение аналогичных действий.

В общем случае включение новых элементов в защищаемый объект всегда приводит к его усложнению, создавая новые структуры факторов, внося дополнительную неопределенность, формируя новые уязвимости и риски, а средства защиты способны не только противодействовать одним угрозам, но и усиливать другие или даже создавать новые.

Еще одно направление, которому не уделяется пока достаточного внимания в теоретическом осмыслении и на практике, связано с преобладанием защитного подхода к обеспечению безопасности. Проблемы в сфере информационной безопасности, например, по-прежнему рассматриваются преимущественно с позиций безопасности информации, которая часто сводится к еще более узкой проблематике – практическим вопросам защиты информации. Ситуация меняется, но в целом подходы к обеспечению безопасности остаются пока преимущественно оборонительными.

Однако за последние годы складывается следующая тенденция: обеспечение безопасности на различных ее уровнях и в разных аспектах приобретает черты противоборства и становится непрерывным процессом. Ориентация лишь на защиту становится недостаточной для поддержания безопасности, технология ее обеспечения требует уже тех или иных атакующих или упреждающих воздействий на потенциального противника. Это обусловлено тотальной информатизацией социо-

и техносферы, всех систем обеспечения жизнедеятельности и управления, самого образа жизни подавляющей части населения, перевод конфликтов в информационное пространство. Даже ставший тривиальным сетевой криминал можно интерпретировать как социотехническое противоборство, а так называемые информационные войны глобального уровня вполне могут быть масштабированы до межкорпоративных конфликтов. Что касается борьбы с террором, то иначе как наступательной она быть не может. При этом информационная и материальная, гуманитарная и технологическая составляющие конфликтов стали неразрывно связанными. Такого рода процессы могут быть описаны и исследованы в терминах динамических моделей.

Первое из обозначенных направлений связано с выявлением профиля риска, т. е. с определением и оценкой значимости некоторого спектра разнородных угроз, не обязательно лежащих в сфере антитеррористической деятельности, с целью выработки наиболее эффективных мер противодействия. И соответствующие данной предметности модели будут сводиться к дискретному оцениванию.

Второе направление предполагает моделирование непрерывных процессов во времени с целью выявления некоторых качественных тенденций или закономерностей, проверку сценариев при вариации начальных условий, коэффициентов, пространства фазовых переменных, представляющих разнородные факторы.

Оба эти направления, внешне разные (в одном случае – оценка состояния, в другом – наблюдение процесса), объединяет то, что объектом исследования являются слабо структурированные, трудно формализуемые системы, с разнородными элементами и плохо измеряемыми показателями. Объединительным для указанных подходов может являться используемое в англоязычной литературе понятие Holistic security.

Разумеется, обозначенные вопросы активно изучаются, обсуждаются, но чаще их анализ сводится к вербальным рассуждениям, не допускающим объективной оценки, когда на всякое обоснованное мнение найдется другое, не худшее и не менее обоснованное. Таким образом, есть потребность в применении формального аппарата, позволяющего пусть не доказать то или иное утверждение или строго обосновать рекомендацию, но, по крайней мере, согласовав базовые положения модели, объективно проверить результаты экспериментов на ней для различных сценариев и начальных условий. Предлагаемые модели в какой-то мере удовлетворяют этим требованиям, показав в эксперименте правдоподобные результаты и потенциальную применимость в исследовании проблем безопасности в различных предметных областях.

В докладе будет представлены основные элементы методики и реализации автоматизированной системы стохастического риск-анализа и

динамической модели противоборства. Полученные на ней некоторые предварительные качественные результаты показали, в частности, что целью противоборства с террористическими организациями, в отличие от отношений с менее агрессивными противниками, может быть только подавление.

Для эффективного противодействия террористическим угрозам необходимо выявление наиболее значимых и актуальных из них, а также их источников, которые могут обнаруживаться далеко от конкретных и конечных проявлений террористической активности или ее организаторов. Видимое решение проблем борьбы с террором может оказать негативное влияние в других сферах жизнедеятельности мегаполисов.

Успешное противодействие угрозам должно непременно включать активную составляющую: защитные мероприятия невозможны без активного противодействия – оборонительная позиция ведут к поражению. При этом активное противодействие не всегда предполагает силовую составляющую, оно может включать организационные меры, экономические, юридические, педагогические и другие вполне мирные средства.

Предложенные формальные методы аналитики в исследовании проблем, порождаемых террористической деятельностью, являются лишь инструментом и не могут заменить традиционные для данной предметной области подходы и методы. Понятно, что модели, построенные для решения конкретных задач, отразят текущий уровень знания (незнания) экспертов, но оценки, получаемые на их основе, по этой же причине будут, по крайней мере, не хуже результатов многовариантного вербального обсуждения, имея при этом преимущество – отсутствие ангажированности и возможность согласования.

УДК 343

А.В. Штрапов

НЕКОТОРЫЕ НАПРАВЛЕНИЯ ИСПОЛЬЗОВАНИЯ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В ДЕЯТЕЛЬНОСТИ ОПЕРАТИВНЫХ ПОДРАЗДЕЛЕНИЙ ОРГАНОВ ВНУТРЕННИХ ДЕЛ

Начало XXI в. характеризуется отчетливо выраженными явлениями глобализации и перехода от индустриального общества к обществу информационному. В настоящее время идет процесс быстрого развития и внедрения компьютерной техники во все сферы человеческой деятельности. Под воздействием научно-технического прогресса повсеместно внедряются новые информационные технологии, которые