АКТУАЛЬНЫЕ ПРОБЛЕМЫ ПРОТИВОДЕЙСТВИЯ ЭКСТРЕМИЗМУ В РОССИИ

Д.ю.н., профессор, заслуженный юрист Российской Федерации В.В. Гордиенко (Академия управления МВД России)

Вступление России в процесс модернизации, то есть коренного преобразования всех сфер общественной жизни в соответствии с национальными интересами и потребностями XXI века, определяет необходимость и дальнейшего развития органов внутренних дел.

Речь идет о пересмотре ряда функций, задач, средств и методов деятельности органов внутренних дел в условиях развития демократии, совершенствования федеративных отношений, радикальных перемен в экономике, культуре и других сферах.

Очевидно, что мы нуждаемся в критическом осмыслении накопленного опыта, как российского, так и зарубежного, в творческом учете исторических, политических и культурных особенностей России, её многонационального, поликонфессионального состава. Нам необходима и творческая смелость в формулировании выводов и рекомендаций.

Актуальность вопросов, вынесенных на обсуждение нашей конференции, определяется рядом обстоятельств.

I. Состоянием противодействия экстремизму в России. Президент Российской Федерации Д.А.Медведев в своем выступлении на расширенном заседании коллегии МВД 6 февраля 2009 г. подчеркнул: «Огромную тревогу за последнее время вызывают проявления экстремизма. В прошлом году на фоне общего снижения преступности количество таких деяний возросло практически на треть. Я не буду говорить простых вещей о том, что Россия многонациональная, многоконфессиональная страна. Такие преступления наносят колоссальный вред, являются системной угрозой существованию нашего общества».

II. Необходимостью анализа деятельности государства и общества, в том числе органов внутренних дел, по противодействию экстремизму во всех формах. Нами накоплен значительный опыт на этом участке обеспечения общественной и государственной безопасности. Данный опыт следует внимательно и всесторонне проанализировать, вскрыть достижения и просчеты, извлечь уроки.

III. Потребностью разработки перспективных направлений совершенствования деятельности органов внутренних дел России по противодействию экстремизму. Страна вступила в новый этап развития, на котором необходимо, концентрировать усилия и ресурсы по превращению страны в мировую державу. Без укрепления общественного порядка и стабильности эти задачи нельзя решить.

Анализ состояния противодействия экстремизму позволяет выделить несколько основных проблем, требующих своего разрешения.

1. Прежде всего, хотелось бы отметить потребность изучения эволюции экстремизма. Изменяется его содержание, формы, а главное – трансформируется характер общественной опасности, исходящей от экстремисткой деятельности.

Экстремизм – сложное, многоплановое явление. В нем соединяются:

а) попытки зарубежных центров подорвать стабильность российского общества, нарушить территориальную целостность Российской федерации.

б) внутренние проблемы нашего развития в сфере политики, экономики, культуры, в области межнациональных и межрелигиозных отношений.

В проблеме противодействия экстремизму концентрируется столкновения двух противоположных явлений:

- с одной стороны, патриотизма;
- с другой – политического авантюризма, агрессивного национализма и религиозной нетерпимости.

Для многонациональной и полирелигиозной России обострение межнациональных и межрелигиозных отношений представляет особую опасность, оно несет опасность раскола и распада страны.

Выдающийся русский мыслитель Владимир Сергеевич Соловьев отмечал: «Всякая народность имеет право жить и свободно развивать свои силы, не нарушая таких же прав других народностей. Это требование равного права для всех народов вносит в политику … высшую нравственную идею которой должно подчиниться национальное себялюбии» (Соловьев В.С. Соч. В 2-х т., I. с.336).

Но лидеры экстремистских структур не желают понять эту простую истину человеческого общежития, они не хотят считаться с достоинством, правами и интересами других народов, с приверженцами иных религий и конфессий.

Усиление агрессивного национализма в ряде регионов России свидетельствует о том, что ксенофобия, т.е. ненависть к другим нациям и народам, публично заявляет о себе.

Национальные интересы России требуют недопущения националистической истерии, решительного пресечения экстремистских акций.

Нам необходимо более детально изучить ряд характеристик современного экстремизма. К ним относятся:

- причины, условия и факторы, стимулирующие развитие экстремизма, его изменения на уровне всей страны, на уровне субъектов Федерации;
- определение «лица», своеобразия экстремизма на региональном уровне, в каждой республике в

составе России, в каждом крае и области.

Например, в ряде республик Северного Кавказа наблюдается усиление позиций религиозно-политического экстремизма, который все активнее вторгается в сферу политических и межнациональных отношений. В краях и областях центральной России популярностью пользуется лозунг: «Россия - для русских!», возрастает «градус» ксенофобии по отношению к мигрантам из ближнего зарубежья, усиливаются позиции ультраправых организаций.

- следует четко определить: какие слои, группы выступают объектом воздействия экстремистских организаций и лидеров; каковы основные лозунги, установки этих организаций.

- более внимательно необходимо проанализировать состав, структуру экстремистских группировок, организаций, лидеров, активистов, их «уличный людской ресурс», способный спровоцировать массовые беспорядки. Ряд индикаторов указывает на то, что ультраправые экстремистские организации располагают значительным влиянием на «улице», они могут создать серьезные проблемы в ряде городов и населенных пунктов Российской Федерации.

Конечно же, в этой связи следует уделить самое серьезное внимание к анализу усиления общественной опасности экстремизма стимулированию межнациональных, межэтнических конфликтов.

По мнению ряда аналитиков, в ряде субъектов Федерации происходит обострение межнациональных отношений. Об этом, в частности, говорит отток русскоязычного населения из республик Северного Кавказа.

2. Серьезной проблемой выступает дальнейшее совершенствование правовых основ деятельности органов внутренних дел по противодействию экстремизму. По мнению значительного, числа работников органов внутренних дел, вызывает множество вопросов юридическая квалификация правонарушений на почве экстремизма.

Например, где проходит грань между точкой зрения конкретного лица, группы, партии и т.д. на ту или иную проблему и возбуждением социальной, расовой, национальной или религиозной розни?

Подобных вопросов существует довольно много. Их нерешенность затрудняет противодействие экстремизму.

Очевидно, назрела необходимость создания постоянно действующих экспертных структур, предназначенных для определения смысловой направленности текстов публикаций, лозунгов, кино-фото-аудио и видеоматериалов. Отсутствие таких структур, поиск научных учреждений в центре и на местах для получения экспертной оценки приводит к серьезным ошибкам и просчетам, к затягиванию сроков расследования.

Перечень проблем, существующих в юридической квалификации правонарушений экстремисткой направленности, можно и нужно продолжать.

Но необходимо находить пути и средства их разрешения.

3. Актуальной проблемой выступает дальнейшая разработка и последовательная реализация комплексного подхода к организации противодействия экстремизму.

Экстремизм порождается «суммой» внешних и внутренних факторов, в том числе экономическими, социально- политическими, культурно- идеологическими и правовыми отношениями.

Следовательно, стратегия противодействия экстремизму призвана охватывать все сферы, начиная от нейтрализации причин и условий его питающих и заканчивая ликвидацией последствий экстремистских акций. Такая стратегия требует комплексного подхода к организации противодействия экстремизму, тесного взаимодействия государственных органов и общественных структур.

Органы внутренних дел – один из субъектов противодействия экстремизму. Они призваны вместе со всеми правоохранительными органами предупреждать и пресекать преступления и административные правонарушения на почве экстремизма.

Применение мер принуждения должно умело сочетаться с действиями органов власти и управления в сфере экономики, политики и культуры. Безусловно, актуальной проблемой выступает повышение эффективности деятельности органов внутренних дел в сфере противодействия экстремизму во всех формах.

4. Совершенствование организации и управления деятельностью органов внутренних дел по предупреждению и пресечению правонарушений экстремистской направленности включает ряд направлений, каждое из которых нуждается в конкретизации.

Прежде всего, необходимо подумать о перераспределении функций и задач между службами и подразделениями органов внутренних дел, как по «вертикали», так и по «горизонтали» с целью устранения дублирования действий направленных на противодействие экстремизму.

Противодействие экстремизму должно быть «адресным», четко обращено к конкретным организациям, группировкам экстремистского толка, предупреждать их воздействие на определенные слои населения и прежде всего – на молодежь.

Основной акцент следует сделать на гибкое сочетание мер профилактики, предупреждения и пресечения.

Очевидно, что одним из основных направлений выступает повышение уровня подготовки сотрудников органов внутренних дел к практическому предупреждению и пресечению правонарушений экстремистской направленности. Часть главных управлений внутренних дел уже разработала свои методические рекомендации по организации и осуществлению противодействия экстремизму. И это оказывает свою помощь работникам органов внутренних дел всех уровней.

Мы нуждаемся также в разработке и внедрении нововведений в организационные и тактические меры

противодействия политическому, националистическому и религиозному экстремизму. В основе этих нововведений может находиться как российский, так и позитивный зарубежный опыт.

5. Следующим направлением повышения эффективности противодействия экстремизму является повышение уровня взаимодействия оперативных подразделений в целях обеспечения своевременной и значимой информацией об экстремистской деятельности лиц, групп, организаций.

Особо хотелось бы подчеркнуть, что действенный механизм предупреждения и пресечения правонарушений на почве экстремизма требует тесного взаимодействия органов внутренних дел со структурами гражданского общества.

Мы еще не сумели повсеместно наладить плодотворного взаимодействия с прогрессивными партиями, общественными организациями, авторитетными общественными и религиозными деятелями в сфере противодействия экстремизму.

Эти прогрессивные структуры способны сдержать и ограничить проявления экстремизма на «глубинном» уровне общества в сфере бытовых, повседневных отношений.

Надо подчеркнуть, что коренные интересы государства и гражданского общества объективно совпадают, ибо права и свободы человека являются высшей ценностью. Их признание, соблюдение и защита – обязанность государства и всего общества.

Владимир Сергеевич Соловьев подчеркивал: «Самое лучшее государство есть то, которое наиболее стеснительно для настоящего реального зла и вместе с тем дает наибольший простор всем силам, двигающим общество к его будущему идеальному благу.») (т.I стр.154).

И мы должны сделать все для «стеснения зла», исходящего от экстремизма. В целях повышения эффективности противодействия экстремизму нам предстоит решить немало проблем.

Основными условиями выполнения этих задач выступают:

- строгая правовая обоснованность действий органов внутренних дел;
- их политическая целесообразность;
- а также высокий профессионализм при предупреждении и пресечении противоправных действий экстремистских группировок и лиц.

ВОПРОСЫ УПРАВЛЕНИЯ ОРГАНАМИ ВНУТРЕННИХ ДЕЛ В БОРЬБЕ С ЭКСТРЕМИЗМОМ В РОССИИ

В.А. Быкадоров (Академия управления МВД России), Г.Ю. Кутузов (Академия управления МВД России)

Строительство в России подлинного правового, демократического и социального государства требует формирование соответствующего государственно-правового и общественно-политического механизма. Поставленную цель можно достичь лишь тогда, когда точно выбраны, выверены и выстроены в систему все его структурные элементы и звенья. Этот процесс становится невозможным вне рамок толерантного сознания всего населения Российской Федерации.

Одной из проблем конституционного развития России на современном этапе является её национально-государственное устройство. Целостность России, её национальная безопасность зависят от единства наций и народностей, проживающих на её территории. Россия является уникальной в мире страной, обладающей неповторимой этнокультурой. Нации и народности, населяющие её, живут на этой территории издревле, что не особенно присуще другим многонациональным государствам мира.

Особенность России заключается не только в её многонациональности, она ещё и многорелигиозна. В России проживают нации и народности - приверженцы различных вероисповеданий. К сожалению, многорелигиозный и многонациональный факторы при неумелом, а порою и преднамеренном их использовании, были и остаются источником напряжённости в России. Этим во многом объясняется множественность и неопределённость понимания духовности, сложность достижения взаимного согласия между народами, отсутствие единой общенародной цели. Это не позволяет успешно решать задачи не только духовной, но и любой другой безопасности человека. Приводит к конфликтам религий и людей, трудностям в управлении государством, религиозному национализму, выражающемуся в вытеснении некоренного населения с территории господствующей религии или нации. Игнорирование указанных факторов приводит к зарождению межнациональной, межрелигиозной напряжённости, неприязни среди населения, перерастающее, как правило, в экстремизм, а в последующем и в терроризм, образуя тем самым реальную угрозу национальной безопасности России[1].

Как известно, под национальной безопасностью России понимается безопасность её многонационального народа как носителя суверенитета и единственного источника власти в Российской Федерации.

Серьёзную угрозу национальной безопасности России представляет экстремизм, проявляющийся в различных формах. При этом национальный, политический и религиозный экстремизм создаёт условия для возникновения конфликтов и непосредственно угрожает федеральному устройству России[2].

В ряде регионов России отмечены попытки раскола по национальному и конфессиональному признаку,

[1] Материал из Википедии – свободной энциклопедии /http://ru.wikipedia.org

[2] Требин М.П. Терроризм в XXI веке. – Мн.: Харвест, 2004 г.

дестабилизации социально-политической ситуации. Это опасный симптом для государства, которое является уникальным национально-территориальным образованием. Ведь в России живут представители 160 национальностей. Между тем если в 2004 году в стране совершено 130 экстремистских преступлений, то в 2008-м - уже 460. Приведенные цифры - данные официальной статистики.[1]

Существенный рост числа межэтнических и межконфессиональных конфликтов в последнее время отмечается и во всем мире. Россия прочно интегрировалась в мировое сообщество, стала открытой страной. И наше общество, естественно, теперь намного восприимчивее к общемировым тенденциям. Как к положительным, так и к негативным. В том числе и к экстремистским настроениям.

Роль управления силами и средствами органов внутренних дел при организации противодействия экстремизму как фактору дестабилизации общественного порядка и общественной безопасности играет главенствующую роль на стадии становления современного общества.

Противодействие экстремистской деятельности основывается на следующих принципах: признание, соблюдение и защита прав и свобод человека и гражданина, а равно законных интересов организаций; законность; гласность; приоритет обеспечения безопасности Российской Федерации; приоритет мер, направленных на предупреждение экстремистской деятельности; сотрудничество государства с общественными и религиозными объединениями, иными организациями, гражданами в противодействии экстремистской деятельности; неотвратимость наказания за осуществление экстремистской деятельности.

Противодействие экстремистской деятельности осуществляется по следующим основным направлениям: принятие профилактических мер, направленных на предупреждение экстремистской деятельности, в том числе на выявление и последующее устранение причин и условий, способствующих осуществлению экстремистской деятельности; выявление, предупреждение и пресечение экстремистской деятельности общественных и религиозных объединений, иных организаций, физических лиц.

В целях противодействия экстремистской деятельности федеральные органы государственной власти, органы государственной власти субъектов Российской Федерации, органы местного самоуправления в пределах своей компетенции в приоритетном порядке осуществляют профилактические, в том числе воспитательные, пропагандистские, меры, направленные на предупреждение экстремистской деятельности.

В условиях глобального мирового финансового кризиса, отразившегося на всех сферах экономики, молодежный экстремизм и безработица среди гастарбайтеров могут стать взрывоопасным коктейлем, по разрушительному потенциалу равным, а в определенных условиях и превосходящим террористическую угрозу. Возросла степень опасности для общества, общественного порядка и безопасности, исходящая от деятельности экстремистских организаций, групп населения; экстремизм способен существенно повлиять на жизнедеятельность России в условиях обострения внутриполитической ситуации, развития негативных процессов в экономике, межнациональных и межрелигиозных отношений[2].

Разработка теоретических и практических методов управления силами и средствами органов внутренних дел при организации противодействия экстремизму как фактору дестабилизации общественного порядка и общественной безопасности основная задача российского государства.

Сообщения о преступлениях доморощенных нацистов стали пугающе привычными. В стране, победившей фашизм, людей избивают и убивают за другой тип лица, цвет кожи, разрез глаз, вероисповедание. Поэтому и потребовалось подразделение, уникальное по своей сути и задачам, специально занимающееся этой не шуточной угрозой.

Особая опасность экстремизма связана и с проявлениями ксенофобии. Имеют место факты дискриминации, насилия на межконфессиональной почве, проявления расизма. Скоординированная деятельность правоохранительных органов с Управлением по надзору за исполнением законов о федеральной безопасности, межнациональных отношениях и противодействии экстремизму Генеральной прокуратуры России, направленная на борьбу с экстремизмом в целом и отдельными его формами - ксенофобией и расовой ненавистью, - призвана способствовать выбору оптимальных средств и методов борьбы с ними. И следовательно, прогнозированию событий и нахождению эффективных путей предупреждения и преодоления этого рода экстремизма[3].

В связи с возникновением выше перечисленных угроз и изменением оперативной обстановки в стране, в 2008 году был образован Департамент по противодействию экстремизму. Спектр экстремистских угроз в нынешнее время разнообразен, но суть его одна - дестабилизация ситуации в стране. При этом зачастую именно молодежь умело используется в противоправных целях. По данным МВД России, количество участников различных движений экстремистской направленности - от националистических организаций до фанатских группировок, находящихся в поле зрения криминальной милиции, - достигает 200 тысяч человек. Кроме того, организованные преступные группировки, расширяя сферы влияния, иногда сознательно придают банальным криминальным разборкам межэтническую окраску[4].

В соответствии с российским законодательством, в том числе с Законом Российской Федерации от 18

[1] Статистические данные. /Официальный сайт МВД России. http://www/mvd.ru

[2] Российская газета. Информационный портал. http://www/Rg.ru

[3] Вахромеев А.В. Международный терроризм и национальная безопасность России // Социально гуманитарные знания – 2004 г.-№ 1

[4] Официальный сайт МВД России. – http://www/mvd.ru

апреля 1991 г. № 1026-1 «О милиции», органы внутренних дел обязаны обеспечивать действующие в стране законы и правосудие, специфическими средствами и методами предотвращать преступления и административные правонарушения, угрожающие личной или общественной безопасности.

В целях повышения качества профилактики и борьбы с преступлениями экстремистской направленности, в части организации управления органами внутренних дел необходимо создание «объединенного банка данных» МВД России об экстремистских формированиях, введение «модели 3-х ступенчатого режима» реагирования органов внутренних дел на общественную опасность, исходящую от действий экстремистской направленности, разработка нового вида специальных операций, т.е. операций по предупреждению и пресечению «комбинированных действий» экстремистских и террористических группировок и организаций, введение в действие Наставления о деятельности служб и подразделений органов внутренних дел по предупреждению и пресечению криминальных проявлений экстремизма, подготовка специальной программы и соответствующих учебно-методических материалов для обучения сотрудников органов внутренних дел навыкам, необходимым при противодействии экстремизму во всех формах.

Совершенствование управления органами внутренних дел при противодействии экстремизму должно реализовываться по двум направлениям.

Первое направление — совершенствование правовых основ деятельности органов внутренних дел по противодействию экстремизму как фактору дестабилизации общественного порядка: изменение модальности Федерального Закона № 114-ФЗ от 25 июля 2002 г. «О противодействии экстремистской деятельности», т.е. его направленности; последовательному применению правовой ответственности за совершение деяний, отнесенных к экстремизму; пересмотр ряда функций субъектов противодействия экстремизму с целью повышения скоординированности их действий; более четкое правовое определение работы по внесению правоохранительными органами представлений в различные структуры.

Особого внимания требует проблема создания специализированных экспертных структур, способных проводить квалифицированную оперативную экспертизу экстремистских действий и материалов. Отсутствие подобных структур резко ограничивает правоприменительную практику.

Второе направление — совершенствование процесса управления органами внутренних дел при противодействии экстремизму как угрозе общественному порядку и общественной безопасности: формирование государственно-общественной системы противодействия экстремизму, в т. ч. более активное участие гражданского общества; создание организационно-правового механизма управления данной системой; обеспечение большей нацеленности на предупреждение и пресечение экстремизма в сфере общественного порядка, которые могут быть «первым звеном» в цепи крупных политических и социальных неконституционных перемен; усиление внимания к профилактической работе в тесном взаимодействии с органами государственной власти, местного самоуправления, с гражданским обществом; повышение эффективности информационно-аналитической работы, в т. ч. создание объединенного банка данных МВД России и ФСБ России об экстремистских организациях; улучшение планирования деятельности органов внутренних дел по противодействию экстремизму в сфере общественного порядка.

Оперативное предупреждение и пресечение таких «комбинированных» действий экстремистских группировок и сил возможно лишь при теснейшем взаимодействии правоохранительных и силовых структур, других органов государства, органов местного самоуправления и активной части общества.

Анализ системы субъектов противодействия экстремизму как фактору дестабилизации общественного порядка и общественной безопасности позволил сделать ряд выводов о том, что в действующей системе противодействия экстремизму в Российской Федерации недостаточное внимание уделяется гражданскому обществу, его структурным элементам в борьбе с этим антиобщественным явлением. Необходимо разработать организационно-правовой механизм управления, который обеспечивал бы координацию деятельности как государственных органов, так и субъектов гражданского общества. Ибо общественный порядок и общественная безопасность - есть результат усилий двух «субъектов»: государства и самого общества и, прежде всего, гражданского общества как его передовой части[1].

Очевидно, что поскольку противодействие экстремизму есть относительно новая, нетрадиционная задача для российских органов внутренних дел, ее решение требует новых знаний, средств, методов, нового опыта по предупреждению и пресечению противоправных действий субъектов экстремистской деятельности; подготовки кадров, способных эффективно управлять подчиненными в сложных ситуациях, готовить и проводить специальные операции по пресечению актов терроризма, массовых беспорядков, межнациональных и межрелигиозных конфликтов, эффективно взаимодействовать с органами государственного управления и субъектами гражданского общества. Особое внимание при этом следует отдавать профилактике экстремистской деятельности, понимать политические и общественные последствия экстремизма.

К ВОПРОСУ ОБ ЭКСТРЕМИСТСКИХ УГРОЗАХ НА ПОТЕНЦИАЛЬНО ВАЖНЫХ ОБЪЕКТАХ ЮЖНОГО ФЕДЕРАЛЬНОГО ОКРУГА

Р.В. Дзгоев (Академия управления МВД России), А.А. Салтыков (Академия управления МВД России)

[1] Колобов О.А. Терроризм и контртерроризм в современном мире: Аналитические материалы, документы, глоссарий: Научно-справочное издание. Экслит, 2003 г.

К настоящему времени во многих регионах России сложилась неблагоприятная обстановка, связанная с ростом риска возникновения чрезвычайных ситуаций техногенного характера.

По данным Ежегодных государственных докладов, современная Россия насчитывает не менее 45 тысяч потенциально опасных объектов различного типа и различной ведомственной подчиненности. В зонах непосредственной угрозы жизни и здоровью в случае возникновения техногенных чрезвычайных ситуаций проживает около 80 млн. человек, т.е. 55 % населения страны.

В частности, как показало изучение информационных и аналитических материалов МЧС России, на территории Южного федерального округа в настоящее время функционирует ряд объектов атомно-энергетического комплекса, среди которых наиболее потенциально опасными для населения и окружающей среды являются Ростовская и Нововоронежская АЭС и химически опасный объект первого класса ОАО «Невинномысский Азот» на котором используются, перерабатываются и хранятся до 20000 тонн хлора и 42000 тонн аммиака.

Особую опасность для населения округа представляют чрезвычайные ситуации, явившиеся следствием террористических актов и экстремистской деятельности. Внимание следует акцентировать на том факте, что тенденция последних пяти лет свидетельствует о значительном повышении доли экстремизма по отношению к террористической деятельности. Экстремистская деятельность помимо мотива оправдания терроризма являет собой крайнюю и активную форму преступной деятельности. Средствами достижения целей такой деятельности могут являться нарушение нормального функционирования объектов повышенной степени опасности, вследствие чего возникает угроза техногенной аварии.

Рассматривая техногенные системы как объекты экстремистской деятельности, особо следует выделить возрастание опасностей в химической промышленности, использующей в производстве химически опасные вещества. Опасность этих веществ для людей обусловлена их способностью, проникая в организм, нарушать его нормальную жизнедеятельность, вызывать различные болезненные состояния, а при определенных условиях – летальный исход. На территории Южного федерального округа размещено 489 объектов, которые используют в производстве более 80 тыс. тонн химически опасных веществ типа хлор, аммиак. В случае чрезвычайных ситуаций на химически опасных объектах наиболее сложная обстановка может сложиться в городах: Волгоград, Волжский, Новочеркасск, Ростов-на-Дону, Каменск-Шахтинский, Волгодонск, Шахты, Краснодар, Кропоткин, Майкоп, Белореченск, Невинномысск, Ставрополь, Махачкала, Нальчик, Владикавказ, Грозный. Катастрофы на таких объектах, как НПО «Азот» г. Невинномысск, ПО «Химпром» г. Волгоград, ПО «Оргсинтез», завод химволокна, завод синтетического каучука г. Волжский могут привести к ЧС регионального масштаба. Кроме того, по железной дороге в границах Северо-Кавказского региона в среднем за сутки перевозится около 3000 тонн АХОВ, в том числе серной кислоты 1300 т, аммиака 1500 т, хлора более 250 т, около 50 тыс. т нефти и нефтепродуктов, а также другие опасные вещества. В случае чрезвычайных ситуаций на железнодорожном транспорте, вызванных действиями экстремистов, наличие этих продуктов усугубит складывающуюся обстановку. Так, при выбросе АХОВ глубина заражения окружающей среды может достигать 80 км, а время стойкости АХОВ – 10 – 12 часов и более.

В целом регион относится к району повышенной опасности воздействия техногенных источников ЧС на население и окружающую среду. Общая площадь территории региона, в пределах которой возможно воздействие поражающих факторов от всех потенциальных источников ЧС, превышает 61 тыс. кв. км, где проживает 43 % населения региона. Как отмечалось выше, в современных условиях резко возросла опасность проведения на перечисленных объектах диверсионных и террористических актов. Статистика свидетельствует, что за последние 10 лет количество преступлений террористического характера и экстремистской направленности на рассматриваемых объектах выросло в несколько раз. Поэтому для защиты потенциально опасных объектов от экстремистской деятельности как источника чрезвычайных ситуаций, следует использовать всю систему государственных мер по обеспечению безопасности. Одним из основных субъектов, привлекаемых к выполнению этих задач, является МВД России. Федеральный орган исполнительной власти в области внутренних дел, его территориальные органы, а также внутренние войска осуществляют физическую защиту и охрану от террористических проявлений значительного числа потенциально опасных объектов. Изучение показало, что к настоящему времени для большинства объектов Южного федерального округа характерна явная недостаточность мер антитеррористической защиты. Дело в том, что на сегодняшний день предметом охранной деятельности является в основном охрана имущества их собственников от преступных посягательств. Даже при успешном выполнении охранных функций, выделяемых сил явно недостаточно для антитеррористической защиты объектов.

Данный вывод следует из результатов проверок состояния антитеррористической защищенности потенциально опасных объектов Южного федерального округа. Эти проверки показывают, что большинство таких объектов охраняются только частной сторожевой охраной. При этом охрана осуществляется, как правило, путем периодического обхода невооруженными охранниками территории объекта. Изучение практики показало, что только на трети исследовавшихся объектов используются средства инженерно-технической укрепленности, специальные средства и служебные собаки, а часть режимных помещений выведена на пульт оператора дежурной смены.

По данным, содержащимся в материалах учения в Южном федеральном округе, из всех потенциально опасных объектов, расположенных на территории округа и не включенных в перечень государственной охраны, только некоторые оборудованы двумя и более системами инженерно-технических средств охраны,

объединенных общим управлением. На части площадных химически опасных объектах первой категории опасности, имевшиеся ранее охраняемые режимные зоны к настоящему времени сокращены в несколько раз.

Опрос специалистов показал, что с переходом собственности из разряда государственной в иные формы, наблюдается тенденция отказа от войсковой системы непосредственной защиты и физической охраны потенциально опасных объектов. Эти изменения влекут уменьшение численности охраны, что в свою очередь, приводит к снижению уровня антитеррористической устойчивости объектов.

На наш взгляд, данную проблему можно решить путем увеличения роли государственных силовых структур в обеспечении охраны потенциально важных объектов. Целесообразно рассмотреть вопрос о передаче под охрану объектов первого класса опасности исключительно в ведение системы МВД России. Также необходимо уделить внимание повышению взаимодействия между правоохранительными органами и частыми охранными структурами в вопросах отражения нападения на потенциально опасные объекты.

Важным условием повышения защищенности рассматриваемых объектов может стать внедрение качественно нового комплекса охранных мероприятий, целью которого станет отражение экстремистских угроз и других противоправных проявлений. Эффективное выполнение указанной цели предполагает, что охранные мероприятия, включая боевые возможности подразделений охраны, инженерно-техническую укрепленность, оборудование техническими средствами обнаружения различных угроз, будут соответствовать определенным государством требованиям.

Таким образом, повышение роли государства в рассматриваемой сфере может стать решающим условием надежной защиты потенциально опасных объектов от экстремистских посягательств.

ГОСУДАРСТВЕННАЯ СИСТЕМА ПРОТИВОДЕЙСТВИЯ ЭКСТРЕМИЗМУ В УСЛОВИЯХ СОВРЕМЕННОГО РОССИЙСКОГО ОБЩЕСТВА

В.А. Епифанцев (Академия управления МВД России), Д.В. Сочнев (Академия управления МВД России)

Государственная система противодействия экстремизму функционирует не столь эффективно, как того требуют реалии сегодняшнего дня. В настоящее время недостаточно скоординированы действия органов государственной власти, в серьезном совершенствовании нуждается система обмена информацией между заинтересованными ведомствами. В общий процесс почти не вовлечены общественные объединения и другие институты гражданского общества.

Сложность и многоплановость проблемы предупреждения экстремизма заключается в том, что во многом в его основе лежат, наряду с кризисными явлениями социально-экономического, политического, духовно-нравственного и иного свойства, проблемы межнациональных отношений. Поэтому здесь необходимы в большей степени не силовые методы воздействия, а соответствующая правовая и экономическая база, подкрепленная социально-психологическими и идеологическими мерами, направленными на ограничение совокупности негативных условий и предпосылок экстремистских проявлений[1].

Требует совершенствования и работа по внесению правоохранительными органами в государственные органы, администрации предприятий, учреждений и организаций, а также в общественные объединения обязательных для исполнения представлений об устранении причин и условий, способствующих возникновению и реализации угроз безопасности Российской Федерации. Такие представления вправе вносить органы следствия и дознания – по материалам конкретных уголовных дел, органы безопасности – в связи с заявлениями и письмами граждан; сообщениями государственных органов, администраций предприятий, учреждений и организаций, общественных объединений, средств массовой информации; результатами оперативно-розыскной деятельности, а органы прокуратуры также – на основании результатов надзорной деятельности.

Тем не менее, невыполнение содержащихся в представлении требований, как правило, существенных правовых последствий для адресата не влечет. Поэтому целесообразно в целях предупреждения экстремистской деятельности предоставить право ряду органов, входящих в государственную систему безопасности, в рамках своей компетенции объявлять должностным лицам или гражданам предостережения о недопустимости нарушения федерального закона.

В настоящее время соответствующие полномочия имеются лишь у органов прокуратуры. Однако в современных условиях, когда правовые возможности по внесению представлений и предостережений не подкреплены никакими карательными санкциями, вынуждающими действительно серьезно относиться к таким формам профилактической работы, эффективность последних, по всей видимости, будет уменьшаться. Поэтому целесообразно также оговорить, что в случае, если непринятие мер по представлению или предостережению послужило причиной или способствовало совершению актов экстремистской деятельности, а также иных преступлений, действия виновных лиц могут быть квалифицированы как преступные в форме повлекшего серьезные последствия неисполнения законного требования прокурора, следователя или иного сотрудника правоохранительных органов.

---

[1] Фридинский С.Н. Некоторые проблемы противодействия экстремизму в Российской Федерации// Прокурорская и следственная практика. – 2006. – №1-2. – С.49-50;Экстремизм и национальный вопрос в России / материалы научно-практического семинара. М.,2009.-С.130-131;Соснин В.А., Нестик Т.А. Современный терроризм: социально-психологический анализ М.,2008.-С.67.

Несомненно, если такие преступления совершены должностным лицом или лицом, занимающим государственную должность Российской Федерации или государственную должность субъекта Федерации, они могут быть квалифицированы как халатность, но проблема заключается в том, что субъектами представлений и предостережений необязательно являются указанные лица – их круг гораздо шире[1].

Важнейшим аспектом для формирования адекватной экстремизму ответной государственной стратегии является рассмотрение не только в криминологическом контексте предупреждения, выявления и пресечения преступлений, но и в целом – в рамках общей системы обеспечения безопасности, представляющей собой многофункциональный и многоуровневый механизм[2].

Необходимо полностью задействовать не только возможности всех органов государственной власти, участвующих в рамках своей компетенции в предупреждении экстремистской деятельности, но также и негосударственных структур, учитывая, что согласно Закону РФ «О безопасности»[3] субъектами обеспечения общественной безопасности являются как государственные, так и негосударственные органы и организации. В настоящее время важной проблемой является развитие взаимоотношений государственных органов в структуре системы безопасности и структур, образующих негосударственную систему обеспечения безопасности в кредитно-финансовой, топливно-энергетической и ряде других сфер. Эта область отношений требует нормативного правового регулирования.

Без должного контроля за развитием конфликтных ситуаций в обществе и возможных проявлений экстремизма, их последствия в форме различных антиконституционных деяний могут стать существенной и реальной угрозой безопасности государства. Соответствующий контроль должен стать многофункциональным (по линии органов внутренних дел, спецслужб, прокуратуры, органов юстиции, религиозных конфессий, общественности и т.д.) и конструктивным – с превентивным корректирующим влиянием на ситуацию.

Как свидетельствует правоохранительная практика, актам экстремизма и ксенофобии обычно предшествуют различные формы протестного, конфликтного, а нередко и насильственного характера. Однако система их раннего предупреждения в настоящее время не создана. Поэтому в целях предупреждения экстремизма и вообще насильственных конфликтов социально-политической направленности должна быть создана государственная система выявления и разрешения таких конфликтов на ранней стадии. Ее задача – осуществление многоуровневого мониторинга и прогноза развития конфликтов как потенциальных угроз безопасности, а также, в перспективе, реализация на данной основе действенного механизма ответственности органов власти различных уровней за принятие не просчитанных по своих последствиям либо умышленных политических, кадровых и административных решений, послуживших причиной социально-политических конфликтов[4].

Необходима именно общефедеральная система прогнозирования и регулирования на ранней стадии социально-политических конфликтов как часть единой государственной системы противодействия экстремизму, включающая не только правоохранительный, но и социальный, экономический, политический и пропагандистский аспекты.

Важнейшее условие борьбы с экстремистскими тенденциями в обществе – создание единой общегосударственной политики противодействия экстремизму. На решение этой проблемы направлена деятельность сформированной в марте 2006 года Объединенной комиссии по национальной политике и взаимоотношениям государства и религиозных объединений. Комиссия представляет собой постоянно действующий консультативный орган при Совете Федерации, призванный способствовать разработке предложений по основам государственной национальной политики и взаимоотношениям органов государственной власти Российской Федерации с религиозными организациями. Единая государственная стратегия по противодействию экстремизму позволит скоординировать действия отдельных государственных структур.

В настоящее время работу по противодействию экстремизму ведут, прежде всего, МВД, силовые структуры и прокуратура. Например, Генеральной прокуратурой принимаются меры по усилению надзора за исполнением законодательства в рассматриваемой сфере по повышению эффективности прокурорского реагирования, включая и организационные. В частности, в сентябре 2006 года в Генеральной прокуратуре создан специальный отдел по надзору за исполнением законодательства о межнациональных отношениях. Данный отдел намерен установить, какие законодательные и исполнительные органы власти занимаются этой проблематикой, в каком объеме, соответствует ли это законодательству и какова система профилактики и предупреждения.

В рамках государственной системы профилактики экстремистских правонарушений Департаментом по противодействию экстремизму МВД России реализуется комплексный план по превентивной деятельности.

---

[1] Устинов В. Создать общественную систему предупреждения и пресечения экстремизма// Российская юстиция. – 2003. – №1. – С. 53-54.

[2] Там же. С. 54.

[3] Закон РФ - № 2446-1 «О безопасности» от 05.03.92 (с изм. и доп. от 25.07.02, 07.03.05) // Российская газета № 103 от 06.05.92.

[4] Стенограмма парламентских слушаний в Совете Федерации «Состояние и проблемы законодательного обеспечения противодействия экстремизму в молодежной среде» от 25 октября 2006 года// Совет Федерации http://www.council.gov.ru.

Однако силовое воздействие на экстремистские группировки не даст никакого эффекта, если одновременно не будет вестись пропаганда выгод и преимуществ национального и политического разнообразия для общественного развития[1].

Информационная составляющая системы предупреждения экстремистской деятельности недостаточно эффективно осуществляет донесение информации обо всем комплексе действующего законодательства России в части противодействия экстремизму и терроризму. Все это в результате приводит к порождению слухов и домыслов, которые полноценно используют деструктивные силы. Поэтому необходимо разработать механизмы, позволяющие сформировать информационное пространство, способное обеспечить доступность для молодежи в получении информации о нормативно-правовой системе России в области противодействия экстремизму.

Следует признать необходимость в российском обществе открытого диалога между правоохранительными органами и молодежной общественностью в вопросах предупреждения экстремизма. Основным результатом отсутствия данного взаимодействия является появление ложных необъективных стереотипов молодежного сознания по отношению к правоохранительным органам. Причем данные стереотипы свое отражение находят в попытках молодежи проявить неуважение к законам государства.[2]

Большим потенциалом антиэкстремистской пропаганды обладает обнародование основных результатов деятельности в сфере противодействия экстремизму. В этой связи представляется целесообразным рассмотреть вопрос о подготовке для печати специального открытого доклада правоохранительных органов о мерах по борьбе с экстремизмом и терроризмом в России. Подобная практика существует, например, в США, ФРГ, Швеции и находит понимание со стороны широких слоев населения.

Отдельного рассмотрения требует проблема противодействия государства религиозному экстремизму, прежде всего, радикальному исламизму, который в большей степени угрожает национальной безопасности страны. Только системное и целенаправленное воздействие органов государственной власти на все подсистемы радикального исламского движения может создать объективные предпосылки для успешной защиты национальных интересов России. Речь идет о выстраивании практических мер по блокированию исламского радикализма, прежде всего его крайних форм; подобные меры можно условно разделить на четыре вида: институционально-правовые, политико-организационные, социально-экономические и административно-силовые[3].

Когда стоит вопрос о формах противодействия различного рода экстремизму, в том числе и под религиозными флагами, это можно сделать только совместно с конфессиями, сверяя позиции, ведя дискуссии. Доминантой взаимодействия государства и религиозных организаций является объединение совместных усилий в целях стабилизации ситуации в обществе, защиты мира и гражданского согласия, решение социальных задач. В данном направлении следует исходить от необходимости подготовки Концепции государственно-конфессиональных отношений[4]. В данном документе отразились бы все изменения в религиозном мире за последние годы, были бы намечены пути совершенствования закона «О свободе совести и религиозных объединениях». Основные направления и приоритеты государственной политики по государственно-церковным отношениям можно сформулировать так: сохранение стабильности конституционного строя; обеспечение гражданского мира и общественного согласия, территориальной целостности; нейтрализация причин и условий, способствующих возникновению конфликтов на религиозной почве. Концепция стала бы своего рода долгосрочной программой работы государства с традиционными и нетрадиционными религиозными объединениями, руководством к действию для чиновников и ориентиром для гражданского общества.

Исследование позволяет сделать следующие выводы:

Противодействие экстремистской деятельности на государственном уровне должно осуществляться по следующим основным направлениям:

– принятие профилактических мер, направленных на предупреждение экстремистской деятельности в молодежной среде ;

– выявление, предупреждение и пресечение экстремистской деятельности общественных и религиозных объединений, иных организаций.

Тенденция переплетения политического и религиозного экстремизма с сепаратизмом представляет собой прямую угрозу конституционному строю и территориальной целостности Российского государства, поэтому задача противодействия экстремизму должна стать неотъемлемой частью общей системы обеспечения национальной безопасности в государстве.

---

[1] Колобов О.А., Сентюрин Ю.П., Сочнев Д.Б., Абышов Р.З. Национал-экстремистские молодежные организации: история и современность: Монография. – Н. Новгород, 2007. – С. 78.

[2] Стенограмма парламентских слушаний в Совете Федерации «Состояние и проблемы законодательного обеспечения противодействия экстремизму в молодежной среде» от 25 октября 2006 года// Совет Федерации http://www.council.gov.ru.

[3] Колобов О.А., Сочнев Д.В., Федорко С.Н. Современные политические технологии противодействия радикальным экстремистским течениям: Монография. – Н. Новгород, 2006. – С.90.

[4] Колобов О.А., Сочнев Д.В., Федорко С.Н. Современные политические технологии противодействия радикальным экстремистским течениям: Монография. – Н.Новгород, 2006. – С. 115.

Наряду с силовым воздействием на экстремистские группировки важнейшим направлением противодействия экстремизму является предупреждение социально-политических конфликтов в обществе и антиэкстремистская пропаганда.

Необходимо развивать информационную составляющую государственной системы противодействия экстремизму, т.е. налаживать информационный обмен между отдельными ведомствами, развивать сотрудничество с представителями СМИ и общественными объединениями в области профилактики экстремизма, устанавливать диалог между правоохранительными органами и общественностью.

Противодействие экстремизму со стороны государства предполагает не только создание единой общегосударственной антиэкстремисткой стратегии, систематизирующей правовые, методологические и организационные нормы пресечения и предупреждения экстремизма, но и развитие экономики, институтов гражданского общества и правового государства.

В системе противодействия экстремизму следует выделить необходимость формирования комплексного подхода к предупреждению политического экстремизма в молодежной среде. Это связано с тем, что рост политического экстремизма в российском обществе все больше охватывает именно российскую молодежь. Сегодня молодежный экстремизм выражается в пренебрежении к действующим в обществе правилам поведения, к закону в целом, появлении неформальных молодежных объединений противоправного характера. Экстремисты нетерпимы к тем гражданам России, которые принадлежат к другим социальным группам, этносам и придерживаются иных политических, правовых, экономических, моральных, эстетических и религиозных идей. Увеличивается опасность появления в скором будущем организованного массового молодежного движения, объединяющего экстремистов, прежде всего, в качестве формы политической борьбы.

Необходимо отметить, что противодействие экстремизму в молодежной среде исключительно силовыми методами МВД, ФСБ и прокуратуры невозможно. Эта задача требует целого комплекса организационных, правовых, профилактических, воспитательных мероприятий, совершенствования взаимодействия государственных органов и общественных организаций.

Тенденция втягивания молодежи в экстремистскую деятельность во многом обусловлена недостаточно эффективной реализацией государственной молодежной политики. Необходимо совместными усилиями государственных органов и общественных организаций наладить систему мониторинга молодежной среды, разработать и принять государственную программу по работе с молодежью.

Наряду с законодательным и организационным регулированием чрезвычайно важным является развитие идеологии толерантности, межнационального согласия, поиска национальной идеи, консолидирующей российское общество, объединяющей все народы многонационального Российского государства, бережного и уважительного отношения к культуре каждого народа.

Важнейшим инструментом противодействия экстремизму в молодежной среде является патриотическое воспитание, которое прививает уважение к государству, всем гражданам страны и национальной идее. В значительной мере на формирование духовно-нравственных ценностей подрастающего поколения влияют средства массовой информации. Они могут и должны играть ведущую роль в формировании мировоззрения молодых людей. Однако общегосударственные информационные системы недостаточно отражают установки на толерантное восприятие различных традиций и ценностей, а информационное законодательство в недостаточной степени защищает интересы детей и молодежи.

МЕСТО СРЕДСТВ МАССОВОЙ ИНФОРМАЦИИ В СИСТЕМЕ ПРОТИВОДЕЙСТВИЯ ТЕРРОРИСТИЧЕСКОЙ ДЕЯТЕЛЬНОСТИ

О.Ю. Кауров (ФГОУ ВПО Кузбасский институт ФСИН России)

На сегодняшний день трудно представить себе человека, живущего без телевизора, интернета, не читающего газет и журналов. Информационный поток, который льется из средств массовой информации (далее – СМИ) оказывает значительное влияние на человеческое мировоззрение. СМИ, как средство формирования общественного климата, давно уже используются людьми, пытающимися путем влияния на группы и слои граждан решить проблемы достижения своих целей, причем не всегда благих. К сожалению, уникальные возможности СМИ также активно используются для достижения целей террористов и экстремистов. Путем освещения в СМИ террористических актов, особенно их последствий, в обществе нагнетается паника, сильно увеличивается общее ощущение уязвимости и страха. Террористам это известно и СМИ активно используются ими, чтобы заранее поставить нас в положение защищающихся.

В 1974 году американский исследователь терроризма Брайан Дженкинс пришел к выводу, что «терроризм - это театр». Абсолютно все террористы, захватывающие заложников, требовали предоставления им права выступить перед представителями средств массовой информации или права выступить в прямом эфире перед телезрителями и радиослушателями. Примерно после 95% совершенных терактов их организаторы звонят в редакции и берут на себя ответственность за совершенное преступление. Террористы, захватывающие заложников, очень часто требуют доставить им телевизоры, радиоприемники и даже свежие газеты, по которым они могут следить за реакцией на свои действия.[1]

[1] См.: СМИ и терроризм: террор стал театром / http://www.temadnya.ru/spravka/17mar2004/3741.html

Из этого следует, что одной из целей террористов является возможность оперативного влияния на общественное сознание, а СМИ – главное средство достижения этой цели.

Террористы всегда стремятся к максимально широкому освещению своих деяний. Эксперты считают, что террористические атаки 11 сентября 2001 года были срежиссированы таким образом, чтобы достичь максимального пропагандистского эффекта. В качестве целей атак были выбраны символы Америки - здание Всемирного торгового центра и Пентагон. Аналогичным образом действовали и многие другие террористические группировки и даже отдельные террористы.[1]

Влияние СМИ, оказываемое на общественное мнение в современном мире, можно назвать ключевым. Сегодня необходимо рассматривать информационную безопасность не только с точки зрения безопасности электронных сетей, связи банков данных, но и с точки зрения безопасности общества от воспевания и героизации насилия и террора в СМИ.[2]

Наибольшую опасность для общества представляет подталкивание (вольное или невольное) СМИ неуравновешенных людей к подражанию действиям террористов путем широкого и неадекватного освещения имеющих место инцидентов. Поэтому работники СМИ, включая редакторов и журналистов, должны оценивать публикуемую ими информацию о подобных происшествиях с точки зрения возможного подражания. А это значит, что в текстах и комментариях информационных сообщений должно отсутствовать описание «технологии» действий террористов и преступников, а также информация, содержащая указания по совершению террористических действий.

Влияние средств массовой информации на нашу жизнь, в том числе на нашу нравственность, огромно, и с каждым днем увеличивается. Лидирующие позиции здесь, конечно, принадлежат телевидению и интернету, ставшими огромной и почти неуправляемой силой. Мы живем в эпоху полного царства телевидения, иными словами в эпоху «тотелеторизма».[3]

Как говорилось выше, очень часто целью террористов является стремление добиться освещения своих действий в СМИ. Утверждение журналистов о том, что они «имеют обязательства представлять аудитории события так, как они происходят, без изъятий и сокращений», позволяют террористам, так режиссировать свои акции, чтобы они наверняка получили всемирное освещение. В этой связи правительствам, законодателям и представителям СМИ необходимо определить свои взаимные права и обязанности с тем, чтобы выработать согласованную политику по недопущению террористов к СМИ, не покушаясь при этом на свободу слова.[4]

Зачастую журналисты, работающие в зоне проведения специальных операций по обезвреживанию террористов, желая как можно подробнее показать весь процесс подготовки и осуществления этих операций, вольно или невольно раскрывают перед широкой аудиторией (а нередко и перед самими террористами) приемы и методы деятельности антитеррористических подразделений.[5] Необходимо выработать профессиональный кодекс для журналистов, которые освещают теракты в прямом эфире, необходима самоцензура у журналистов, ведущих репортаж. Самоцензура, конечно же, представляет собой идеальный вариант, требующий наличие высокой нравственности как у самих журналистов и средств массовой информации, так и у всего общества в целом. Бесспорно, добиться таких результатов мгновенно не представляется возможным.

В этой связи, прибегнув к методу государственного (законодательного) регулирования, можно предложить дополнить Уголовный кодекс статьей 205.3 «Распространение сведений о специальных средствах, технических приемах и тактике проведения антитеррористических операций». В ст. 4 Федерального закона «О средствах массовой информации»[6] уже содержится данное условие, однако, нарушители остаются безнаказанными. Данная норма позволит привлекать таких нарушителей к уголовной ответственности.

Практика показывает, что только легитимное, то есть рассматриваемое как законное, оправданное в глазах общества применение силы может быть эффективным в борьбе с терроризмом. Если же общественное мнение не только не понимает, зачем против террористов применяется насилие, но и сочувствует им, трудно достичь победы в борьбе с терроризмом. Поэтому в СМИ необходимо убедительно доказать обоснованность использования силы против террористов, раскрывать опасность и антигуманную сущность терроризма, дегероизировать его вождей и исполнителей. Констатация требований террористов должна быть свободна от риторики и пропаганды. Идеально, если они будут перефразированы, и если им будут даны соответствующие правовые комментарии и оценки.

Таким образом, надо полагать, что залогом успеха при предотвращении последствий террористических актов является конструктивное сотрудничество СМИ и органов правопорядка и власти.

---

[1] См.: СМИ и терроризм: террор стал театром / http://www.temadnya.ru/spravka/17mar2004/3741.html

[2] См.: Вартанова Е.Л. Круглый стол «Борьба с терроризмом и свобода слова» / http://www.mediascope.ru/node/45

[3] См.: Боровик Г.А. Круглый стол «Борьба с терроризмом и свобода слова» / http://www.mediascope.ru/node/45

[4] См.: Хлобустов О.М. О роли СМИ в противодействии терроризму / http://terroristica.info/node/336

[5] См.: Петрищев В.Е. Заметки о терроризме. М., 2001. С. 97-98.

[6] См.: Закон РФ от 27.12.1991 № 2124-1 (ред. от 25.12.2008) «О средствах массовой информации»// Российская газета, № 32, 08.02.1992

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ОБЪЕКТОВ С МАССОВЫМ ПРЕБЫВАНИЕМ ЛЮДЕЙ

А.В. Кузьмин (Академия управления МВД России), А.В. Михайлов (Академия управления МВД России), Ж.З. Омаева (Академия управления МВД России)

1. Все мы, кто понаслышке, кто из средств массовой информации, а кто-то, возможно, как непосредственный очевидец, знаем, что происходит на стадионах во время матчей и как ведут себя болельщики после, если их команда вдруг неожиданно потерпела поражение. Разъяренные толпы людей бегут и сметают все со своего пути. Болельщики – это не единственная опасность, которая может случиться. Все так же знают и помнят о слове «терроризм». Одной из сфер, где терроризм проявляет высокую активность, является международный спорт. Теракт может произойти в любом месте массового скопления людей, в том числе и в спортивном сооружении.

Данное положение объясняется тем, что международные спортивные мероприятия привлекают значительный общественный интерес и одновременно в них участвуют большие массы людей. Влияние террористов на международный спорт может приобретать различные формы.

Самым характерным примером международных спортивных мероприятий как цели террористов могут служить Олимпийские игры. Особую актуальность политические проблемы противодействия терроризму в сфере международного спорта приобретают в связи с получением Россией права на проведение в 2014 г. зимних Олимпийских игр в Сочи. Поэтому изучение аспектов противодействия терроризму в сфере международного спорта представляется весьма важным не только в теоретическом, но и в практическом смысле.

2. При подготовке и проведении зимних Олимпийских игр 2014 г. в Сочи потенциально существует ряд террористических угроз, различаемых по степени опасности. К ним можно отнести недовольство части населения Сочи в связи с его отселением в другие районы, беспокойство экологических неправительственных организаций по поводу возможности нанесения ущерба природе. Существенное значение с точки зрения обеспечения безопасности имеет напряженная обстановка в Северокавказском регионе и ситуация вокруг Абхазии. Все эти факторы должны быть в поле зрения российского государства.

В настоящее время именно ООН является ведущей международной организацией, в рамках которой осуществляется координация контртеррористической деятельности на глобальном уровне. На глобальном уровне имеется тринадцать принятых в рамках ООН универсальных конвенций и протоколов к ним по борьбе с различными проявлениями терроризма, большинство из которых вступили в силу. Все тринадцать конвенций и протоколов к ним являются универсальными, они касаются всего мирового сообщества, в той или иной степени затрагивают самые важные аспекты обеспечения безопасности людей.

В рамках ООН серьезное внимание уделяется проблемам противодействия терроризму в сфере международного спорта. Так, в 2003 г. в системе ООН был создан Международный постоянно действующий орган по наблюдению за мерами безопасности при проведении важнейших политических событий (МЕПДОН). К важным политическим событиям МЕПДОН относит Олимпийские игры, встречи на высшем уровне и массовые мероприятия. По тематике безопасности Олимпийских игр проводятся специальные семинары, научно-практические конференции.

К Олимпийским играм обычно привлечено внимание сотен миллионов человек на всех континентах. Если вместо того, чтобы увидеть высшие достижения человеческой воли и духа, зрители станут свидетелями кровавой драмы, как это было в Мюнхене в 1972 г., то террористы рассматривали бы такое достижение как исполнение своих самых смелых замыслов. Из других терактов на Олимпийских играх можно вспомнить события в Атланте (США) в 1996 г., когда от взрыва бомбы 1 человек погиб и 110 получили ранения. Террористы угрожали и другим спортивным соревнованиям самого высокого уровня. Например, террористы ИРА провели теракт во время первенства Европы по футболу в Манчестере в 1996 г.

3. Рассмотрение опыта контртеррористического обеспечения предыдущих Олимпиад создает определенные возможности для более качественной подготовки к Олимпиаде в Сочи. Одновременно возникает вопрос о том, насколько имевшие место в прошлом угрозы могут иметь место в будущем. Кроме того, существует возможность возникновения новых угроз, которые пока еще не проявили себя. Наиболее вероятно, что при проведении Сочинской Олимпиады наряду с типичными угрозами будут присутствовать и особенные, присущие только ей. Одной из таких проблем является потенциальная возможность бойкота Олимпиады в Сочи. При подготовке Олимпиады в Сочи необходимо иметь в виду и ряд других обстоятельств в сфере контртеррористической деятельности, которые могут препятствовать успешному проведению Игр. Хотя зимние Олимпийские игры составляют всего примерно треть масштаба летних игр по видам спорта и количеству участников, они находятся в таком же центре мирового общественного внимания, как и летние игры. Нельзя сказать, что Кубань в целом, и Сочи в частности, являются спокойным регионом. В Южном федеральном округе в 2006 г. было совершено более 700 преступлений террористического характера, из которых - свыше ста терактов. Хотя количество преступлений террористической направленности снизилось на 42%, тем не менее, оно остается весьма значительным.

4. Для предотвращения потенциальных вспышек насилия и проведения террористических акций необходимы, проводить следующие меры на стадионах, а именно:

а) стремиться, чтобы конструкция стадионом гарантировала безопасность зрителей, позволяла осуществлять эффективный контроль за их поведением, способствовала вмешательству служб безопасности и сил правопорядка;

б) осуществлять дифференциацию болельщиков соперничающих команд, резервируя для болельщиков-гостей и болельщиков-хозяев - если -это допустимо и возможно - разные трибуны;

в) обеспечивать эту дифференциацию, строго контролируя продажу билетов, и принимать особые меры предосторожности в период, непосредственно предшествующих матчу;

г) исключать доступ на стадионы и матчи, когда это юридически возможно, известным или потенциальным зачинщикам беспорядков и лицам в состоянии алкогольного или наркотического опьянения;

д) оснащать стадионы эффективными системами связи со зрителями и контролировать их эффективное использование, а также снабжать зрителей программами матчей и другими проспектами, чтобы добиться от них корректного поведения;

е) запрещать пронос зрителями на стадионы алкогольных напитков; ограничивать, а еще лучше запрещать продажу алкогольных напитков на стадионах и обеспечивать, чтобы напитки продавались в безопасных емкостях;

ж) обеспечивать специальный контроль с целью помешать зрителям, вносить на стадион предметы, могущие служить средством насилия, или пиротехнические средства;

з) обеспечивать сотрудничество с заинтересованными властями в том, что касается мер, которые следует принять, чтобы контролировать поведение зрителей и применять надлежащие правила с помощью согласованных действий.

Все эти обстоятельства необходимо учитывать при подготовке к Сочинской олимпиаде.

ЗАРУБЕЖНЫЙ ОПЫТ ВОЕНИЗИРОВАННЫХ ФОРМИРОВАНИЙ В БОРЬБЕ С ТЕРРОРИЗМОМ

А.Ю. Манцуров (Дальневосточный юридический институт МВД России)

Международный экстремизм и его вечные спутники — терроризм и сепаратизм бросили реальный вызов всему цивилизованному сообществу. Террористические атаки, проведенные Аль-Кайдой в отношении США, Великобритании, Испании, Индонезии и Индии заставили по иному смотреть на ту борьбу, которую вела и ведёт Российская Федерация против международного терроризма в Чечне.

В 2006 году в Российской Федерации был принят кардинально новый нормативно-правовой акт - Федеральный закон от 6 марта 2006 г. № 35-ФЗ «О противодействии терроризму»[1]. Именно с этого момента борьба с терроризмом в России перешла на качественно новый уровень – была создана единая антитеррористическая система. Так в соответствии с Указом Президента РФ от 15 февраля 2006 года № 116 «О мерах по противодействию терроризму»[2], в целях совершенствования государственного управления в области противодействия терроризму образован Национальный антитеррористический комитет.

На основании данных нормативно-правовых актов внесены существенные изменения в Федеральный закон от 6 февраля 1997 года N 27-ФЗ «О внутренних войсках МВД Российской Федерации», направленные на расширение антитеррористических полномочий войск.

В связи с этим особую значимость приобретает зарубежный опыт военизированных формирований, обеспечивающих внутригосударственную безопасность, накопленный ими в деле борьбы с терроризмом.

Конечно, безусловный приоритет при решении задач обеспечения общественной безопасности во всех демократических странах отдается исключительно ненасильственным силам и средствам. Однако история развития человечества не знает механизмов обеспечения правопорядка и спокойствия в стране только ненасильственными методами. Необходимыми элементами системы обеспечения внутренней безопасности любого демократического государства являются полиция и вооруженные силы, находящиеся под контролем органов государственной власти и действующие в рамках, предоставленных им национальным и международным законодательством.

Вооруженные силы демократического государства в его повседневной жизни в охране правопорядка практически не используются (исключение из этого правила составляют страны, имеющие в составе своих полицейских сил особый их вид – жандармерию: Франция, Италия и др. вооруженную полицию: КНР, Япония и др.).

Но при осложнении оперативной обстановки в сфере охраны правопорядка внутри государства картина резко меняется. В кризисных ситуациях любое демократическое государство и не только немедленно использует вооруженные силы для нормализации обстановки в стране.

Так в Великобритания 38 лет длилась операция «Знамя» (с 1969 года и по 1 августа 2007 года в шести графствах одной из составных частей Соединённого Королевства – Северной Ирландии, на постоянной основе несли службу по охране общественного порядка вооружённые силы страны, в том числе элитные части

[1] ФЗ от 06 марта 2006 г. № 35-ФЗ «О противодействию терроризму» (С изм. и доп. ФЗ от 30 декабря 2008 г. N 321-ФЗ) // СЗ РФ от 13.03.2006, N 11, ст. 1146.

[2] Указ Президента РФ от15.02.2006 г. № 116 «О мерах по противодействию терроризму» (с изм. и доп. Указ Президента РФ от 4 июня 2009 г. N 631) // СЗ РФ от 20.02.2006, N 8, ст. 897.

воздушно-десантных войск, так как полиция собственными силами была не в состоянии обеспечить режим комендантского часа и предотвратить межконфессиональные столкновения между католиками и протестантами)[1].

Во Франции в 1995 году после серии террористических актов, в результате которых погибло 10 человек и около 200 получили ранения, был введен специально разработанный на случай чрезвычайных обстоятельств план «Вижипират». По этому плану патрулирование всех улиц крупных городов и станций метро, а также повсеместная проверка документов у населения осуществлялась совместными нарядами армии, полиции и жандармерии в течение четырех месяцев – до поимки руководителей и наиболее активных членов террористических групп. Части и подразделения регулярных вооруженных сил (в дополнение к силам и средствам полиции и жандармерии) широко использовались и во время проведения летом 1998 года во Франции чемпионата мира по футболу[2].

В Соединенных Штатах вооруженные силы традиционно широко применяются при урегулировании кризисных ситуаций внутри страны. В частности, при подавлении массовых беспорядков в городе Лос-Анджелесе в 1992 году, кроме сил полиции самым активным образом использовалась заранее отмобилизованная дивизия Национальной Гвардии и бригада морской пехоты – элитное соединение вооруженных сил США. В результате, в течении нескольких суток порядок в городе был восстановлен, при этом свыше полусотни человек было убито, 2116 человек получили ранения[3]. Помимо этого, Террористические акции произошли во время Олимпийских игр в Лос-Анджелесе (1984 г.) и Атланте (1996 г.). Последствия этих актов были достаточно ограниченными в силу широкомасштабных операций по предупреждению действий террористов во время массовых международных мероприятий.

Так, в июле 1984 г. за несколько недель до начала XXIII Олимпийских игр в Лос-Анджелесе правительства некоторых азиатских государств получили по почте угрозы в адрес своих атлетов. Как выяснилось, эти послания были разосланы одной из организаций ку-клукс-клана, базирующейся в штате Вирджиния. Министерство обороны США в связи с этим затратило почти 800 млн. долларов на обеспечение безопасности спортсменов при проведении спортивных мероприятий. В частности были задействованы 77 вертолетов для ведения разведки, наблюдения и медицинской эвакуации.

Практика проведения террористами своих акций во время массовых мероприятий, установившаяся в последнее десятилетие XX столетия, обусловила принятие американским военным ведомством мер по предупреждению терактов еще до начала Олимпийских игр в Атланте в 1996г.

В соответствии с американскими уставами и другими подзаконными актами была развернута система военной поддержки Олимпийских игр. Министр армии (сухопутных войск) был назначен главным координатором всех военных программ поддержки от министерства обороны США. Для выполнения этой задачи ему была подчинена группировка войск, состоявшая из частей и подразделений регулярной армии и Национальной гвардии, численностью до 10 тыс. человек. Военнослужащим была поставлена задача оказать помощь патрульной полиции штата Джорджия, полицейскому управлению города Атланты и другим правоохранительным органам, осуществить военную поддержку их мероприятий по поддержанию общественного порядка и безопасности во время проведения игр.

Организация предупредительных антитеррористических мероприятий на Олимпийских играх в Атланте началась за полтора года до них (в первые месяцы 1995 г.). В разработке мероприятий приняли участие, кроме офицеров ФБР, представители Секретной службы (отвечает за охрану американского президента), Бюро по алкоголю, табаку и огнестрельному оружию, полиции штата Джорджия, управления полиции города Атланты, управления полиции графства Фултон.

В Китайской Народной Республике с конца 80-х годов войска Вооруженной народной полиции неоднократно привлекались для подавления выступления китайского населения в крупных городах, в том числе в мае-июне 1989 г. в г. Пекине на площади Тяньаньмэнь, вызвавшего всемирный протест.

В Джакарте (Индонезия) 5 августа 2003 года произошел взрыв в гостинице «Мариотт». Погибли 12 человек и около 150 получили ранения. Теракт совершила «Джамаа Исламийя» - исламская суннитская экстремистская организация. Правительство Индонезии на экстренном заседании приняло решение о введении в стране дополнительных мер безопасности, были привлечены вооруженные силы для поддержания общественного порядка.

Во Франции при проведении мероприятий по предупреждению террористических акций и при так называемых рядовых серийных акциях террористов в мирное время вооруженные силы выступают обычно как второй эшелон и средство обеспечения и усиления правоохранительных органов и специализированных антитеррористических подразделений (таких, как специальные подразделения французской жандармерии).

Так, в целях предупреждения возможных террористических актов при проведении массовых мероприятий в связи с подготовкой встречи нового века, в качестве предупредительной меры министр внутренних дел Франции приказал, начиная с 24 декабря и всю следующую неделю до первых дней января

[1] См.: А.В.Быков. Теоретические и прикладные проблемы функционирования национальных полицейских систем. Дис... доктора юрид. наук, М., 2008. С.32.

[2] Там же. С. 32.

[3] И.М.Попов, А.В.Быков. А.В. Губанов. А.В. Капкин. Внутренние войска (структуры им подобные) в системе обеспечения внутренней безопасности зарубежных государств (1945-1997 гг.). М., 1998. с.13.

2000 г., держать в режиме боевой готовности две трети всего личного состава полицейских и жандармов, а также некоторые подразделения сухопутных войск. Всего было привлечено до 70 тыс. человек.

Большинство западноевропейских и азиатских государств ярко реагируют на все проявления экстремистской деятельности, и как правило, организовывают специальные вооруженные формирования по ее противодействию.

Например, в Испании в 1978 году, по примеру немецкого антитеррористического спецназа GSG-9, в составе корпуса полиции был создан спецназ Grupo Especial para los Operaciones (GEO) как полицейский антитеррористический блок, в который приходят на службу лучшие специалисты спецслужб Испании.

Для проведения диверсионных, контртеррористических операций и урегулирования внутригосударственных конфликтов в начале 50-х годов в Великобритании были созданы так называемые войска специального назначения.

В Китае в начале 80-х годов подразделения сил быстрого реагирования были введены в состав сухопутных войск, ВВС, и ВМС, а также в состав армейской авиации, морской пехоты, воздушно-десантных войск и войск специального назначения. Под влиянием уроков военной операции объединенных сил в Персидском Заливе, в 1992 году были созданы специальные силы под названием «Мобильные Боевые Силы» (МБС) для разрешения критических ситуаций, которые подчиняются непосредственно Центральной Военной Комиссии (ЦВК) КПК.

В целом богатый зарубежный опыт обеспечения внутригосударственной безопасности посредством применения внутренних войск или структур им подобных и вооруженных сил заслуживает тщательного изучения и учета в деятельности отечественных структур, обеспечивающих внутреннюю безопасность Российской Федерации на современном этапе.

ОСВОБОЖДЕНИЕ ЗАЛОЖНИКОВ: ОРГАНИЗАЦИОННЫЕ И ТАКТИЧЕСКИЕ АСПЕКТЫ

Т.И. Мовлаева (Академия управления МВД России)

1.С каждым годом расширяется круг деяний представляющих, несомненную опасность для страны, в частности, террористические акции, связанные с захватом заложника. Без глубокого анализа, без разработки методики и тактики проведения различных организационных и тактических мероприятий правоохранительные органы не могут бороться с этими преступлениями и будут постоянно отставать от преступников.

2.В подготовке и совершении такого рода преступлений можно выделить ряд этапов: формирование группы преступников, распределение ролей; сбор информации о намеченной жертве или ее близких. Преступные группы используют информаторов из числа работников коммерческих структур, в отношении которых намечаются преступное вымогательство; разработка детального плана захвата или похищения с учетом раннее полученной информации, подготовка места дальнейшего сокрытия похищенного человека; непосредственный захват или похищение человека; действия преступников по получению выкупа и освобождение ими заложника в том числе силами органов внутренних дел.

3.При освобождении заложников и похищенных людей и задержании лиц, их захвативших, важна первичная информация. Можно выделить два момента, когда на стадии получения информации органы внутренних дел: ничего не знают ни о лицах, совершивших похищение, ни о требованиях, которые они хотят выдвинуть; имеют сведения (возможно, приблизительные) о преступниках (какие-либо телефоны, номера автомашин, адреса, само содержание требования, место и время его выполнения).

4.При проведении комплекса мероприятий по освобождению заложников необходимо делать ставку на так называемый контактный обмен, т.е. возврат похищенного в обмен на то что, что требуют преступники. Последнее является важным во всех случаях без исключения при проведении подобных операций. В противном случае вероятность освобождения человека живым сводится к минимуму, так как он является свидетелем, видевшим преступников, знающим, где они находятся, и может их изобличить. Поэтому необходимо идти на всевозможные уловки, «уступки», постараться «вывести» преступников на «контактный » обмен. При разработке планов операции по освобождению заложников необходимо иметь несколько вариантов продолжения, а не полагаться только на какой- то один вариант. Когда же все задействованные варианты работают без срывов и взаимодополняют друг друга, то это приводит к благополучному во всех отношениях завершению операции.

5.Неотъемлемым и наиболее важным элементом организации и тактики освобождения заложника является ведение переговоров. Практика накопила большой опыт, в частности в стилях ведения переговоров: мягкая позиция, жесткая позиция и принципиальные переговоры.

Стили ведения переговоров

Мягкая позиция	Жесткая позиция	Принципиальные переговоры
Участники переговоров- друзья	Участники переговоров - противники	Участники переговоров – партнеры в решении проблемы.
Цель-соглашение	Цель- победа	Цель - эффективное и бесконфликтное решение проблемы
Быть мягким к людям и проблеме	Быть жестким к проблеме и людям	Быть мягким к людям, жестким к проблеме

Доверять другим	Не доверять другим	Освободиться от доверия или недоверия
Легко менять позицию	Твердо стоять на своих позициях	Сосредоточиться не на позиции, а на интересах
Вносить предложения	Угрожать	Изучать интересы
Раскрыть свою позицию	Вводить в заблуждение в отношении своей позиции	Не иметь твердой позиции
Принять односторонние потери в целях достижения соглашения	Требовать односторонних преимуществ в качестве условия достижения соглашения	Учитывать возможности взаимной выгоды
Искать единственно возможный ответ, приемлемый для другой стороны	Искать единственно возможный ответ, приемлемый для себя	Выбирать ответ из различных вариантов
Настаивать на соглашении	Настаивать на своей позиции	Настаивать на использовании объективных критериев
Пытаться избежать волевой борьбы	Стремиться к победе в волевой борьбе	Пытаться достичь результата, основанного на нормах, не зависимых от воли сторон
Сдавать позиции под давлением	Оказывать давление	Аргументировать и выслушивать аргументы, подчиняться не давлению , а принципу

МЕРЫ И ВРЕМЕННЫЕ ОГРАНИЧЕНИЯ ПО ЗАКОНОДАТЕЛЬСТВУ РЕСПУБЛИКИ ТАДЖИКИСТАН, ПРИМЕНЯЕМЫЕ ПРИ ВИДЕНИИ ЧРЕЗВЫЧАЙНОГО ПОЛОЖЕНИЯ

Д.К. Норов (Академия Управления МВД России)

В современной отечественной и зарубежной литературе по проблеме прав человека вопрос их ограничения, в том числе правового, получил определенное отражение в исследованиях многих представителей общеправовой теории и науки конституционного права. Заметим, что в ней наблюдается разнообразие подходов к пониманию категории «ограничение».

Так, правовые ограничения рассматриваются в качестве способа правового регулирования общественных отношений.[1]

С.С. Алексеев же считает, что ограничения – это вопрос не о способах, а об объеме регулирования, о границах имеющихся у лиц прав, которые характеризуют результат юридического регулирования.[2]

Наиболее глубоко проблему правовых ограничений исследовал А.В. Малько, который рассматривает правовое ограничение как правовое сдерживание противозаконного деяния, создающее условие для удовлетворения интересов контр субъекта и общественных интересов в охране и защите.[3]

Понятие «ограничение прав и свобод» стало непосредственным предметом теоретического анализа «круглого стола» на тему: «Принципы, пределы, основания ограничения прав и свобод человека по российскому законодательству и международному праву», проводившегося журналом «Государство и право» в 1998г »[4]

В выступлениях М.И. Байтина, Н.Н. Вопленко, В.И. Гоймана, А.М. Нагорной, В.А. Толстика и других теоретиков права данное понятие было раскрыто в самых разных контекстах, хотя общего мнения относительно единообразной и оптимальной трактовки определения, все-таки, достигнуто не было.

«Ограничение права (свободы), - по мнению В.И. Гоймана, - это осуществляемое в соответствии с предусмотренными законом основаниями и в установленном порядке сужение его объема»[5].

М.А. Нагорная считает, что ограничения прав человека представляют собой изменение содержания или объема действия нормы права. В международных актах правомерность ограничений признается на определенных основаниях и с благими целями (ст.29 Всеобщей декларации прав человека). В России они противостоят гарантиям прав человека и касаются конституционных прав.[6]

---

[1] Братько А.Г. Запреты в советском праве. Саратов, 1979. С.17; Козюк М.Н. Правовое равенство и привилегия депутатской неприкосновенности // Личность и власть. Ростов-на-Дону, 1995. С.165.

[2] Алексеев С.С. Общие дозволения и общие запреты в советском праве. М., 1989. С.65.

[3] Малько А.В. Стимулы и ограничения в праве. Теоретико-информационный аспект. Саратов, 1994. С.60; Он же – Правовые ограничения: от отраслевого ограничения к теоретическому // Правоведение. 1993. №5 С.19.

[4] Принципы, пределы, основания ограничения прав и свобод человека по российскому законодательству и международному праву // Государство и право. 1998. № 7,8,10.

[5] Принципы, пределы, основания ограничения прав и свобод человека по российскому законодательству и международному праву // Государство и право. 1998. №10. С.26-27.

[6] Там же. С. 36.

Пробел теоретической не проработанности проблематики ограничения прав и свобод в период действия особых правовых режимов был восполнен С.В. Пчелинцевым, в монографии[1] которого представлено теоретическое осмысление оснований, целей, принципов, пределов и содержания ограничения прав и свобод человека и гражданина в таких условиях.

Сущность ограничений прав и свобод граждан в условиях особых правовых режимов, по его мнению, заключается в приостановлении действия ряда прав и свобод как меры временного характера, применяющейся в виде законодательно установленных ограничений и запретов совершения определенных действий, введении дополнительных обязанностей и выражающейся в сокращении (сужении) общего объема прав и свобод граждан, затрагивающих их статус.[2]

Правомерное ограничение административно-правового статуса граждан, выступая в качестве средства реализации режима чрезвычайного положения, послужило основанием выделения особой формы административно-правового регулирования. Ее специфика в характере правового воздействия на отношения в условиях чрезвычайного положения и выражается в установлении режима административно-правовых ограничений.

Расширение компетенции органов управления дает им возможность определенным образом изменить характер принудительного воздействия на граждан и юридических лиц. Действие предписаний об ограничении прав и свобод в условиях чрезвычайного положения распространяется не на конкретных лиц, а на население всей данной территории.

Ограничения чрезвычайного положения относятся к административно-правовым, поскольку в качестве средств их составляющих выступают административно-правовые запреты, обязывания и дозволения , на основе которых возникают правоотношения с участием субъекта исполнительной власти в сфере общественной безопасности. В конкретных социальных отношениях эти правоограничения выражаются в виде специальных управленческих мер, применяемых субъектами исполнительной власти.

Мера-это средство достижения какого-либо результата.[3] Категория «чрезвычайные меры» в широком понимании может рассматриваться как совокупность административно-правовых и организационно управленческих действий, совершаемых органами исполнительной власти в условиях чрезвычайного положения, основной целевой направленностью которых является ограничение отдельных прав и свобод граждан. На институциональном уровне юридическая конструкция чрезвычайной меры представляет собой предписание, адресованное, с одной стороны, гражданам и организациям, обязывая их претерпевать соответствующие правоограничения, а с другой, содержит дозволение, позволяющее исполнительным органам осуществлять действия по реализации правоограничений.

Таким образом, под чрезвычайными мерами будем понимать вызванную чрезвычайной ситуацией управленческую деятельность, выраженную в предусмотренных законом юридических формах и направленную на установление и поддержание режимных правил поведения, форм особого управления и на создание условий, препятствующих возникновению и развитию угрозы безопасности. В данном случае термин «чрезвычайные» означает, что данные меры могут применяться только в условиях чрезвычайного положения; по содержанию представляют собой ограничения прав и свобод граждан, наложение на них дополнительных обязанностей; изменение полномочий и функций органов государственной власти и местного самоуправления. Правоограничительные меры выступают юридическим элементом управления чрезвычайной ситуацией.

По целевому назначению предусмотренные законом меры и временные ограничения условно можно объединить в отдельные группы, направленные на предупреждение нарушений общественного порядка и режима чрезвычайного положения (предупредительные и запретительные меры); выявление правонарушений; обеспечение нормальной жизнедеятельности населения (меры, усиливающие охрану общественного порядка); обеспечение гарантий прав граждан и организаций.

Согласно ст.4 Конституционного Закона Республики Таджикистан « О правовом режиме чрезвычайного положения » от 10 мая 2002г. под №134. к основным мерам и временным ограничениям, применяемым при введении чрезвычайного положения, относятся:[4]

1). Усиливать охрану общественного порядка и объектов,

обеспечивающих жизнедеятельность населения и народного хозяйства;

2). Временно выселять граждан из районов опасных для проживания , с обязательным предоставление им стационарных или временных других жилых помещений;

3). Вводить особый режим въезда и выезда граждан;

4). Запрещать отдельным гражданам покидать на условленный срок определенную местность, свою квартиру (дом), выдворять нарушителей общественного порядка не являющихся жителям данной

[1] Пчелинцев С.В. Проблемы ограничения прав и свобод граждан в условиях особых правовых режимов. – М.: Норма, 2006.

[2] Пчелинцев С.В. Указ. Соч. С.436.

[3] Ожегов С.И. Словарь русского языка. М., 1989. С.349.

[4] Конституционный Закон Республики Таджикистан « О правовом режиме чрезвычайного положения » (в редакции закона от 10.05.2002, от 28.12.2005г. №134).

местности, за их счет к месту своего пребывания или за пределы местности, где объявлено чрезвычайное положение;

5). Временно изымать у граждан огнестрельное и холодное оружие и боеприпасы, а у предприятий, учреждений и организаций также и учебную военную технику, взрывчатые, радиоактивные вещества и материалы, сильнодействующие химические и ядовитые вещества;

6). Запрещать проведение собраний, митингов, уличных шествий и демонстраций, по своему содержанию влияющих на дестабилизацию обстановки, а также публичных голодовок и пикетирований, зрелищных, спортивных и других массовых мероприятий;

Подобная мера обусловлена тем, что как свидетельствует практика, митинги, демонстрации и иные массовые мероприятия экстремистски настроенные лица используют в своих корыстных целях и провоцируют собравшихся на групповые нарушения общественного порядка, которые, как правило, перерастают в массовые беспорядки, блокирование либо захват особо важных объектов и совершение иных насильственных общественно опасных действий. Так, 12 февраля 1990г. в Душанбе экстремисты с целью захвата власти, используя проходивший перед зданием ЦК митинг, спровоцировали вначале нападение на это здание, а затем массовые беспорядки перешли и в жилые микрорайоны города, в результате которых погибли 23 человека, десятки ранены, было повреждено, сожжено и разграблено более 100 объектов торговли, госучреждений, городу был нанесен огромный материальный ущерб.[1] Только благодаря введенному чрезвычайному положению и применению запрета на проведение демонстраций, собраний, манифестаций, забастовок, стачек, производственного саботажа в городе удалось силами правопорядка пресечь попытки проведения новых митингов и взять обстановку под свой контроль;

7). Устанавливать особый режим работы предприятий учреждений и организаций независимо от формы собственности, а также решать другие вопросы их хозяйственной деятельности;

8). Назначать и освобождать от должности руководителей предприятий, учреждений и организаций, запрещать увольнение рабочих и служащих по уважительным причинам;

9). Использовать ресурсы предприятий, учреждений и организаций для предотвращения и ликвидации последствий чрезвычайных обстоятельств с последующей выплатой компенсации в порядке, определяемом Правительством Республики Таджикистан;

10). Запрещать проведение забастовок;

11). Привлекать трудоспособных граждан для работы на предприятиях, в учреждениях и организациях, а также для ликвидации последствий чрезвычайных обстоятельств, обеспечивая безопасность труда;

12). Ограничивать или запрещать торговлю оружием, боеприпасами, взрывчатыми, сильнодействующими химическими и ядовитыми веществами, за исключением лекарственных препаратов;

13). Вводить карантин и проводить другие обязательные санитарно – противоэпидемические мероприятия;

14). Ограничивать или запрещать использование множительной техники, а также радиопередающей аппаратуры, аудио и видеозаписывающей техники, изымать звукоусиливающие технические средства, устанавливать контроль за средствами массовой информации , при необходимости вводить цензуру ограничения на выпуск газет;

15). Вводить особые правила пользования связью;

16). Ограничивать движения транспортных средств и проводить их досмотр;

17). Вводить комендантский час;

18). Пресекать создание и деятельность вооруженных формирований граждан, не предусмотренных законодательством Республики Таджикистан.

19). Проверять документы граждан, а в необходимых случаях, применяющихся данных о наличии у граждан оружия. Боеприпасов, взрывчатых, сильнодействующих химических и ядовитых веществ, проводить личный досмотр, досмотр веществ и транспортных средств.

20). Запрещать ввоз и вывоз с целью распространения в других местностях печатных изданий магнитофонных и видеозаписей призывающих по своему содержанию к дестабилизации обстановки, разжиганию межнациональной розни, неповиновению органам государственной власти и управления.

Таким образом, перечисленные меры и временные ограничения в своей совокупности составляют правовой режим чрезвычайного положения, который по своему содержанию носит двойственный, противоречивый характер. С одной стороны, меры и временные ограничения служат средством устранения чрезвычайных, кризисных ситуаций и восстановления нормальных, обычных условий жизнедеятельности населения в определенных границах, а с другой – чрезвычайные меры связаны с объективной необходимостью принятия экстраординарных мер, ограничивающих суверенитет личности и меняющий содержание социального управления.

Для устранения обстоятельств, послуживших основанием для введения чрезвычайного положения, меры и временные ограничения могут применяться по Указу Президента Республики Таджикистан в полном или частичном объеме.

[1] Известия. 1990. 15 марта.

Как отмечает А.Э. Жалинский, введение чрезвычайного положения, во многом связано с проблемой ответственности, которая может порождаться действиями, вызвавшими необходимость в особом режиме, а также противодействием порядку чрезвычайного положения, либо превышением власти в этой ситуации, либо халатностью или некомпетентностью власти. Эта ответственность может носить политический, государственно–правовой и иной характер.[1]

Определенная ответственность за введение чрезвычайного положения и, следовательно, правомерность применяемых мер и временных ограничений в соответствии с Конституцией Р.Т. ложится на Президента Республики Таджикистан, который уполномочен вводить чрезвычайное положение, и Маджлиси Оли, утверждающий Указ Президента о введении чрезвычайного положения.

Важно отметить, что перечень мер и временных ограничений, предусмотренный КЗРТ от 10 мая 2002г., сложился не сразу. В ряде случаев перечень мер и временных ограничений дополнялся новыми мерами. Так, чрезвычайное положение, введенное в сентябре 1988г. в Нагорно-Карабахской автономной области и Агдамском районе Азербайджанской ССР, не предусматривало мер изоляции лиц, нарушающих общественный порядок и своими действиями разжигающими национальную рознь. Но затем, учитывая обострение обстановки в Азербайджанской ССР, Президиум Верховного Совета СССР своим постановлением от 23 ноября 1988г. « О неотложных мерах по наведению общественного порядка в Азербайджанской ССР и Армянской ССР» предоставил право должностным лицам ОВД в местностях, где было введено ЧП (установлен комендантский час), задерживать в административном порядке таких лиц на срок до 30 суток с их содержанием в спецприемниках.

Указом Президиума Верховного Совета СССР от 15 января 1990г. « Об объявлении чрезвычайного положения в Нагорно-Карабахской автономной области и некоторых других районах» правовой режим был дополнен нормой и приостановлении противоречащей закону деятельности организаций и самодеятельных объединений граждан или роспуске их.

Указ Президиума Верховного Совета Таджикской ССР от 12 февраля 1990г. «Об объявлении чрезвычайного положения в г. Душанбе» ввел ответственность лиц, нарушивших комендантский час.[2]

Эти и другие нормы были учтены при принятии в СССР Закона от 3 апреля 1990г. «О правовом режиме чрезвычайного положения», а затем и законами Республики Таджикистан 1994 и 2002гг.

КОММУНИКАЦИОННЫЕ ТЕХНОЛОГИИ ПРОТИВОДЕЙСТВИЯ ИДЕОЛОГИИ ТЕРРОРИЗМА И ЭКСТРЕМИЗМА

Г.К. Овруцкая (Южный федеральный университет, г. Ростов-на-Дону)

Полагаем, что эффективная борьба с терроризмом и экстремизмом невозможна без идеологического противодействия, организованного в виде коммуникационных сообщений транслируемых через каналы средств массовой коммуникации. На наш взгляд, содержание информационных продуктов представляет собой набор идеологических конструкций, с помощью которых субъекты массовой коммуникационной деятельности оказывают влияние на массовое сознание.

Важным этапом в изучении идеологии можно считать то, что современные исследователи перестали воспринимать ее как данность, а показали ее «конструируемость» при помощи различных культурных практик. Это дискурсивная концепция идеологии (концептуализация идеологии по модели языка), согласно которой идеология представляет собой множество смысловых конструкций, но не четко сформулированные доктрины. Процесс конструирования идеологии происходит через создание иллюзии «естественности» происходящего в сообщениях СМК и вызывании эффекта «сопричастности» и «сопереживания» людям и событиям. По выражению К.Гирца, «...идеология преобразует чувство в значение и предоставляет его в распоряжение социума»[3].

Таким образом, идеология действует минуя сознание индивида. Однако исследователи отмечают, что хотя на первый взгляд идеология формирует человека «спонтанного», но в действительности, эта спонтанность является идеологической иллюзией, необходимой для воспроизводства социального порядка[4].

Анализ Интернет-среды показывает, что в виртуальной среде ведется массированное идеологическое воздействие, пропаганда идеологии экстремизма и терроризма. Так, например, популярный молодежный ресурс http://www.youtube.com содержит сотни роликов откровенного экстремистского содержания, имеющих высокий рейтинг просмотра.

Выполненные в жанре социальной рекламы, эти ролики подготавливают массовое сознание к принятию экстремистских идей, формируют соответствующие социальные представления, облегчают процесс

[1] Жалинский А.Э. Правовой статус населения в условиях чрезвычайного положения // Обеспечение безопасности населения и территорий. - М., 1994. С.27.

[2] М.П. Киреев, В.И. Севрюков, С.А. Семейкин. Правовые и организационные основы управления силами и средствами при введении чрезвычайного положения. М., 2003г.

[3] Гирц Клиффорд. Идеология как культурная система // Новое литературное обозрение. № 29. 1998 г. с.17.

[4] Рисмухамедов И.А. Концепция идеологии А. Грамши и Л. Альтюссера и их рецепция в современном неомарксизме. Автореферат диссертации на соискание ученой степени кандидата социологических наук. Санкт-Петербургский государственный университет. 2003.

группообразования, активизируют антисоциальную активность населения. Очевидно также, что массовое сознание, технологично обработанное подобным образом, является залогом эффективного рекрутинга в экстремистские группы, обеспечивает членам последних социальную поддержку за счет легитимизации соответствующих практик. В общем виде подобное массовое медийное воздействие является составной частью террористических и экстремистских практик, фактором их эффективного функционирования.

Идеология терроризма и экстремизма - сложный феномен, требующий методологии междисциплинарного исследования и выработки системных практик по противодействию данной идеологии. Ведь идеология терроризма и экстремизма, реализуясь в области массового сознания предполагает воздействие на определенные социальные группы, активное формирование таких групп. С этой целью используются, в том числе, и массовые коммуникации. Применительно к практикам противодействия экстремизма и терроризма целесообразно организовать системную работу по информированию различных социальных групп о сути этой идеологии, о её негативных следствиях; специальной системной деятельности по социальной профилактике, социальной терапии и социальной реабилитации.

Полагаем, что данные цели могут быть максимально эффективно решены в жанре социальной рекламы. Согласно ст. 18 Федерального закона «О рекламе», социальная реклама определяется как деятельность по представлению общественных и государственных интересов, направленная на достижение благотворительных целей. Стратегически социальная реклама может формировать адекватные социальные представления об экстремизме и терроризме, задавать мировоззренческие установки, формировать социально желательные виды поведения (бдительность, готовность оказывать помощь правоохранительным структурам, конструктивное поведение в экстремальных ситуациях и т.д.).

Целенаправленное осуществление социального влияния с целью изменения общества «в лучшую» сторону и, тем самым осуществление профилактики и управления социальными конфликтами происходило на протяжении всей истории развития человечества. Сначала в виде обычаев, традиций, морали и нравственных ценностей. Затем все вышеупомянутое сводилось в рамки различных религиозных систем. С развитием индустриального общества и возникновением феномена массовой коммуникации, функция «воспитания» масс переходит от традиционных методов распространения социальных и религиозных норм к новым инструментам – массовым коммуникационным технологиям – пропаганде, агитации, ПР, рекламе.

Несмотря на достаточно широко очерчиваемый законодательством спектр субъектов социальной рекламы от граждан до юридических лиц, практика социального рекламирования в России укладывается в рамки патерналистского подхода: коммуникатор - государство, реципиент – общество. Считаем, что в нашей стране, к сожалению, до сих пор доминирующими социальными представлениями в этом плане являются представления о том, что борьба с терроризмом и экстремизмом является деятельностью сугубо государственной, выполняемой только силовыми органами. Экстремизм и терроризм представлен в массовом сознании как исключительно «исламский», а пресловутый «чеченский след» является наиболее распространенной атрибуцией в «наивном» объяснении трагических событий.

Подобная ситуация является благоприятной почвой для развития идеологии экстремизма. Представленные в открытом доступе экстремистские медиатексты можно классифицировать на следующие группы:

1. Артикуляция той или иной социальной проблемы как межнациональной, межрасовой, межрелигиозной и требующей радикальных, гуманистически ориентированных, разумных и всем понятных действий (например, предвыборный ролик партии «Родина» «Очистим наш город от мусора»[1]).

2. Оправдание, легитимизация и героизация экстремистских и/или террористических практик (например, ролик на песню Т. Муцураева «Галерея памяти - шахиды в судный день»).

3. Формирование негативных установок относительно той или иной национальной, расовой, религиозной или иной социальной группы (например, ролики на тему трагических событий в Кондопоге).

4. Формирование лояльности к определенным экстремистским действиям (организация материальной и иной помощи экстремистским движениям, формирование потребности в получении дополнительной информации). К такому типу относится, например, реклама, продвигающая экстремистские сайты.

5. Означивание тех или иных социальных событий в рамках экстремистской идеологии.

6. Формирование групп и повышение их сплоченности (например, реклама по продвижению субкультуры скинхедов).

7. Реклама, напоминающая и активизирующая экстремистские действия (например, реклама, инициирующая принять участия в «Русском марше»).

Представленная же в наши дни в Интернет-сети отечественная реклама, направленная на противодействие идеологии экстремизма и терроризма, немногочисленна и, в основном, направлена на формирование толерантности в межнациональных отношениях. В ней практически отсутствуют рекламные обращения, формирующие общую антитеррористическую и антиэкстремистскую идеологию (в общем виде идеологию гуманистическую). По сути, не отработаны такие важные её темы, как формирование конструктивных действий в экстремальных ситуациях, профилактика, коррекция и терапия экстремистского сознания, продержка положительного образа правоохранительных органов, группообразование и поддержка групп социально активной молодежи, референтных лидеров, способных активно и эффективно противостоять

[1] Здесь и далее в качестве примеров приводятся ролики с сайта http://www.youtube.com

экстремистским нормам и т.д. Практически не используются для этих целей каналы подростковых и молодежных субкультур (анимэ, готы, панки, байкеры и др.). Делать это особенно важно, так как указанные и подобные им молодёжные субкультуры в своем идеологическом корпусе обладают различным уровнем экстремизма и, конечно же, требуют грамотного, системного социального контроля и активной нюансированной коррекции. Такое воздействие должно быть релевантным целевым аудиториям по своему внешнему содержанию и по форме подачи. В наибольшей степени, на наш взгляд, последнему условию соответствует социальная реклама, распространяемая посредством сети Интернет.

Таким образом, социальную рекламу можно рассматривать как востребованный способ противодействия идеологии терроризма и экстремизма. Ее целесообразно использовать на уровне социальной профилактики, коррекции и социальной реабилитации.

СОВРЕМЕННЫЕ ПРОБЛЕМЫ БОРЬБЫ С ЭКСТРЕМИЗМОМ В РОССИИ

А.В. Павлинов (Владимирский юридический институт ФСИН России)

В настоящее время экстремизм все чаще именуют синонимом «преступления вражды и ненависти». Использование данного термина вызвано несколькими моментами. Во-первых, изменением дефиниции «экстремистская деятельность» в новой редакции закона «О противодействии экстремистской деятельности», содержащей слагаемую «совершение преступлений по мотивам, указанным в пункте «е» части первой статьи 63 Уголовного кодекса Российской Федерации». Во-вторых, зарубежным опытом борьбы с экстремизмом.

Сомнение в обоснованности такого наполнения и однозначного понимания прежнего термина неизбежно вызывает вопросы.

Во всех ли слагаемых экстремисткой деятельности данная мотивация присутствует?

Далеко не для всех она обязательна. Например, обусловленность насильственного изменения основ конституционного строя, оправдания терроризма и иной террористической деятельности может быть и иной. В подобном поведении скорее доминирует месть, самоутверждение, корыстная или иная личная заинтересованность, теократическая жажда власти.

Как разрешить мотивационный дуализм в некоторых общеуголовных преступлениях и правонарушениях, содержащих помимо конститутивной уголовно-правовой мотивации и мотивацию ненависти и вражды?

В чью пользу в таких преступлениях как хулиганство, изнасилование, уничтожение или повреждение чужого имущества должна быть разрешена конкуренция различных побудительных начал?

Из вышеперечисленного следует, что мотивация вражды и ненависти не является безусловным интегративным критерием, обязательным признаком проявлений экстремизма. Необходимы какие-то иные объединяющие признаки либо синонимы экстремизма как родового понятия конгломерата противоправного поведения. Лишь для этнорелигиозного экстремизма – это, скорее всего обязательный мотив.

Поэтому только система характерных, устойчивых признаков способна образовать и отразить такое явление как экстремизм.

Доминирование экономических причин экстремизма

Основное отличие экстремизма и преступлений на почве вражды и ненависти проявляется и в круге детерминантных факторов.

Результаты исследования, проведенного крупными научными центрами по изучению причин межэтнической нетерпимости, презентация которого состоялась в Общественной палате РФ весной 2009 года, указали на то, что социально экономические условия не влияют на формирование межнациональной нетерпимости.[1]

В свою очередь социально экономические реалии на проявления антигосударственного экстремизма оказывают существенное влияние. Они катализируют процессы легитимной смены власти, инициируют и способствуют достижению целей «оранжевых революций», являются непременными детерминантами насильственного изменения основ конституционного строя. Мы продолжаем утверждать, что причины наиболее опасной формы экстремизма - антигосударственного экстремизма на юге России лежат, прежде всего, не в сфере психологии, этнической ментальности, радикализации национального фактора, а в плоскости прежних ошибок политического руководства, социально-экономическом кризисе, свободном обороте оружия и распространении радикальной исламистской идеологии.[2] Теперь к ним добавилась, как известно, и тотальная коррупция. Ранее сложившийся стереотип отсталого в экономическом положении региона Северного Кавказа не только не преодолен, но и стал еще резче выраженным в связи с углубившейся дифференциацией в развитии всех регионов страны.

---

[1] См.: отчет о научно-практическом семинаре "Экстремизм и национальный вопрос в России", проведенном в Государственной Думе Российской Федерации 28 мая 2009 г. Комитетом по безопасности и Национальным Антикриминальным и Антитеррористическим Фондом // http: // www.waaf.ru/ index_ru. php?section=7&paragraph=11&article=4

[2] См.: А.В.Павлинов. Криминальный антигосударственный экстремизм: уголовно-правовые и криминологические аспекты. Автореф. дисс. на соиск. … док. юрид. наук. – М., 2008. С.12.

Нам представлялось большим заблуждением считать и во многом такое заблуждение сегодня преодолено, что чеченский вооруженный конфликт (1994 - 1996 гг.) явился порождением и следствием межнациональных, религиозных, этнотерриториальных противоречий. Как отмечалось в постановление Правительства РФ в 1996 г. основными причинами возникновения и существования чеченского кризиса явились экономические (финансовые) интересы различных криминально-клановых группировок в Чечне, связанных с банковско-финансовыми структурами, как в России, так и в других странах СНГ, стремление чеченского руководства к достижению «полной» независимости от федерального центра. С опорой на незаконные вооруженные формирования у политических лидеров Чечни появилась возможность диктовать свои условия и решать эти стратегические задачи. Одна из современных тенденций – аппеляция лидеров незаконных вооруженных формирований, проявляющих активность в стремлении к самоопределению на юге России, к той части международного сообщества, которое рассчитывает на обретение доступа к источникам энергетических ресурсов России.

Таким образом, антигосударственный экстремизм в сфере национально-государственных отношений сепаратистской направленности, точно также как и антигосударственный экстремизм в социально-политической сфере радикально-оппозиционной направленности детерминирован экономическими факторами.

И приоритетные меры его профилактики, как отмечается в стратегических документах, направленных на борьбу с преступностью данного вида, и которые наиболее интенсивно реализуются на практике – проведение ярко выраженной социально - направленной экономической политики.

Так в условиях усиления социальной направленности современной экономической политики функцию общественных фондов потребления в текущий период должен взять на себя Государственный резервный фонд. В 2009 году показатели социальных выплат (пенсионерам, др. категориям) превысят показатели инфляции. Рост расходов государства на социальную политику в 2010 году в России составит более 10 процентов. Межбюджетные трансферты из федерального бюджета в 2008 - 2009 году достигли (в млрд. руб.): Карачаево-Черкессия – 20,7, Ингушетия - 30,7, Кабардино-Балкария – 31,9, Дагестан – 107,4, Чечня - 180,2. Всего - 350,9.[1] Необходимо не только федеральное софинансирование социальных и инвестиционных программ регионов, в т.ч. путем принятия дополнительной федеральной целевой программы развития юга России, но и жесткий контроль за их выполнением.

Стратегия национальной безопасности Российской Федерации до 2020 года (Стратегия) и Концепция долгосрочного социально-экономического развития Российской Федерации на период до 2020 года (Концепция) отмечают взаимосвязь между уровнем экономического развития регионов и состоянием национальной безопасности.

В частности в ст.64 Стратегии указывается на необходимость «сокращения уровня межрегиональной дифференциации в социально-экономическом развитии субъектов Российской Федерации путем сбалансированного территориального развития.

В долгосрочной перспективе угрозы национальной безопасности, связанные с диспропорцией уровней развития регионов России, предотвращаются путем развертывания полномасштабной национальной инновационной системы за счет формирования перспективных территориально-промышленных районов в южных регионах … и в других регионах Российской Федерации».

В преамбуле раздела VII. «Региональное развитие» Концепции также подчеркивается, что «государственная региональная политика направлена на … сокращение дифференциации в уровне и качестве жизни населения в регионах с помощью эффективных механизмов социальной и бюджетной политики».

На социально-экономический фактор, как основной в комплексе причин и условий, порождающих одну из наиболее опасных форм экстремизма – терроризм указывает и Концепция противодействия терроризму.[2]

Пусть не прямо, но в п.в) ст.1 Концепции подчеркивается основная современная тенденция проявлений крайних форм политически мотивированного насилия, обусловленная внутренними политическими, экономическими, социальными факторами. Однако далее Концепция снова акцентирует внимание на межэтнических, межконфессиональных факторах.

В одном из выступлений президента РФ Д.Медведева подчеркивалась политическая некорректность терминов «исламский», «религиозный» экстремизм.[3]

Последние события в Ингушетии, Дагестане, Чечне (весны - лета 2009, зимы 2010 г.), связанные с посягательствами на представителей местной власти скорее обусловлены именно «иными социальными противоречиями» (см. п.а) ст.3 Концепции), но не межэтническими, не межконфессиональными.

Основные внешние факторы, способствующие возникновению и распространению терроризма в Российской Федерации, перечислены в статье 4 Концепции. О внешнем факторе чаще всего говорят «силовики» и руководители регионов (президент Ингушетии Ю.Евкуров). Иная позиция звучит из уст Президента РФ о том, что экстремизм на Северном Кавказе обусловлен внутренними противоречиями: бедностью, коррупцией.

---

[1] См.: Центр фискальной политики. Расчеты программы «Диалог». Телеканал РБК. 22 января 2010 года.

[2] См.: Концепция противодействия терроризму в Российской Федерации (утв. Указом Президента Российской Федерации 5 октября 2009 г.) // Российская газета от 20 октября 2009 г.

[3] Д.. Медведев предлагает заменить «исламский экстремизм» на исламский телевизионный канал // http: // www.islam.ru/ rus/ 2009-08-28/ ? single =28216

Современные проблемы законодательного регулирования экстремизма

За рубежом нет политизации экстремизма. До прихода мирового финансово-экономического кризиса политические потрясения в виде антигосударственного экстремизма в развитых постиндустриальных странах практически отсутствовали вовсе либо давно ушли в прошлое. Имела место лишь ксенофобия в форме расизма и национализма. Государственная власть в развитых странах устойчива, ее смена осуществляется в цивилизованной форме через выборы, политическая борьба проходит в законодательно оформленном русле, гражданское общество сформировалось, функционирующая экономика способна обеспечить все население высоким материальным уровнем жизни. Государства, испытывающие периоды становления демократических режимов, социально-политические и экономические кризисы, как Россия, страны ближнего зарубежья, особенно Центрально-азиатского региона, подвержены проявлениям насильственного антигосударственного экстремизма. Тектонические сдвиги в платформе национально-государственного устройства ставят в опасность их территориальную целостность и единство, суверенитет.

С середины первого десятилетия 21 столетия на юге России и к концу его в странах западной Европы стали все более доминировать экономические и политические факторы проявляющегося антигосударственного экстремизма.

Вместе с тем поправки, внесенные Федеральным законом №111 от 24.07.2007 г., не служат консолидации общества, еще более обостряют существующие противоречия.

Поэтому следует согласиться с позицией В.В.Лунеева о порочности политизации бытовых преступлений, таких как хулиганство, вандализм, клевета и о необходимости исключить социальную, политическую, идеологическую ненависть или вражду как отягчающее обстоятельство из ряда статей УК РФ (ст.105 ч.2, ст.111 ч.2, ст.112 ч.2 и др). [1] Соответственно из п. «е» ч.1 ст.63 УК РФ необходимо исключить «политическую, идеологическую ненависть и вражду», «мотив ненависти и вражды в отношении какой-либо социальной группы» как обстоятельство, отягчающее наказание. Статью же 282 УК РФ следует оставить в прежнем виде за исключением признака «а равно принадлежности к какой-либо социальной группе» или его переформулировать.

После такой реконструкции в остатке останется: насильственный антигосударственный экстремизм и экстремизм ксенофобского толка.

Реальной тенденцией современной российской уголовной политики, которая наряду с гуманизацией также может быть преобладающей в ближайшее время, стало наращивание законодательного обеспечения, превентивно-карательного потенциала, прежде всего УК, в борьбе с наиболее опасными формами экстремизма. Учитывая повышенную общественную опасность, масштаб и чудовищность последствий таких преступлений для общества и государства, сохраняющуюся угрозу единству, территориальной целостности Российской Федерацией мы предлагаем в борьбе с экстремистской деятельностью (ее крайними формами, такими как терроризм):

- продолжить выработку предложений об оптимизации уголовной ответственности за счет реализации превентивно-карательного потенциала УК РФ, использования технико–юридических средств дифференциации уголовной ответственности и индивидуализации (ужесточения) наказания, в т.ч. за счет комплекса дополнений институтов и норм Общей части Уголовного Кодекса РФ;

- изменение основного закона для обуздания преступности данного вида как диктуют того чрезвычайные ситуации и последующее появление в УК РФ норм – исключений, отступлений от прежних конституционных положений. Отдельные радикальные изменения в УК также возможны и в рамках предписаний ч.3 ст.55 Конституции РФ.

Сразу следует оговориться: предлагаемые нами изменения находятся где-то посередине между тем, что есть на текущий момент в УК РФ и другим крайним полюсом, когда речь заходит о применении чрезвычайных мер в отношении данных преступников. Для ликвидации террористов «без эмоций и колебаний» сотрудникам спецслужб нужны и правовые основания, правовые рамки функционирующего режима контртеррористической операции. [2]

На современном этапе остается актуальным системный пересмотр УК и УПК с целью повышения эффективности ресурсного обеспечения борьбы с проявлениями терроризма и других форм насильственного антигосударственного экстремизма, в т.ч. путем наращивания карательного воздействия. Это коррелирует с инициативами руководителей государства и правоохранительных органов. Так, глава Следственного комитета при Генеральной прокуратуре РФ А.Бастрыкин на коллегии своего ведомства заявил, что вообще нельзя досрочно выпускать на волю террористов, организаторов преступных групп.[3] Президент РФ Д.Медведев выступил с предложением изменить территориальную подсудность по уголовным делам террористического и экстремистского характера и изъять из подсудности суда с участием присяжных заседателей дела, касающиеся преступных сообществ и организованных преступных группировок.[4]

---

[1] См. В.В.Лунеев. Российский экстремизм: политика и реалии // Криминологический журнал Байкальского государственного университета экономики и права. №3 (9), 2009.

[2] См.: А.В.Павлинов Стратегия борьбы с насильственным антигосударственным экстремизмом и преступностью в условиях современной России. – М.: Издательство «Юрлитинформ», 2010.

[3] См.: Особо опасных не выпускать // Российская газета от 13 февраля 2009 года. С.4.

[4] См.: Ликвидация без эмоций. Дмитрий Медведев провел совещание по нейтрализации террористических и экстремистских

Как убедительно доказывают исследования, история общего предупреждения, а вместе с ним и история уголовного наказания не представляют собой непрерывного прогресса от замены негуманных средств социального контроля на более гуманные.[1] Актуальна и ныне проблема соответствия суровости наказания размеру и характеру вреда, причиненного преступлением, проблема обеспечения неотвратимости полноценного наказания.

Несмотря на идеальные представления социалистического правосознания о надлежащей суровости, огромное желание руководителей появившегося первого в мире социалистического государства ограничить репрессию (террор) «минимальнейшим минимумом»[2] в первые годы своего существования Советская власть в условиях постоянной террористической угрозы, перманентных проявлений насильственного антигосударственного экстремизма, гражданской войны была вынуждена дважды после нескольких отказов вводить смертную казнь.[3]

Безусловна аналогия с текущим моментом: отказываться от крайних мер уголовной репрессии (смертная казнь, исключение применения гуманистических институтов и норм Общей части в т.ч. условно-досрочного освобождения от наказания, амнистии, помилования) в отношении наиболее опасных проявлений экстремизма преждевременно.

Появление смертной казни как действующего вида наказания несоразмерно понижает мотивирующее значение лишения свободы лишь в случае недостаточно репрессивного значения последней. В нынешних условиях существования максимального наказания за совершение единичного преступления в виде 20 лет лишения свободы, по совокупности преступлений и приговоров 25 и 30 лет лишения свободы и существования пожизненного лишения свободы такого понижения не произойдет.

Переходным мостиком между смертной казнью и лишением свободы на длительный срок, пожизненным лишением свободы могут стать предлагаемые нормы – исключения. Кстати и исключительная мера наказания в такой ситуации перестанет быть исключительной.

О НЕКОТОРЫХ МЕРАХ ПО СОВЕРШЕНСТВОВАНИЮ ФЕДЕРАЛЬНОГО ЗАКОНА «О ПРОТИВОДЕЙСТВИИ ТЕРРОРИЗМУ»

Д.Н. Рачев (Академия управления МВД России), Э.В. Стариков (Академия управления МВД России), М.П. Киреев (Академия управления МВД России)

В 2006 году в Российской Федерации были приняты новые федеральные законы и указы Президента Российской Федерации, которые изменили государственную политику участия правоохранительных органов нашей страны в выявлении, предупреждении, пресечении и минимизации последствий актов терроризма. Хочу показать Вам, уважаемые коллеги, схему, на которой и отображено сегодняшнее состояние организации, а также участия органов внутренних дел МВД России в процессе противодействия и борьбы с преступлениями террористического характера (схема № 1).

Заметим, что в целом, изменения государственной системы противодействия терроризму в Российской Федерации коснулись передачи всей полноты ответственности Национальному Антитеррористическому комитету, что, безусловно, является положительным, однако, такой подход, по нашему мнению, снижает уровень организации государственных органов по такому важному направлению деятельности. В первую очередь, я имею ввиду отстранение Правительства нашей страны от прямого участия в делах НАК. По ранее действовавшему законодательству Председатель Правительства возглавлял Федеральную Антитеррористическую комиссию РФ, что, безусловно, придавало комиссии высокий статус и ее решения были «безусловно» обязательны для министерств, служб и агентств Российской Федерации, участвующих в выявлении, предупреждении и пресечении терроризма.

Другими концептуальными недостатками действующего антитеррористического законодательства Российской Федерации являются:

1. «Размытость» определения понятия «терроризм», содержащегося в ст. 1 Федерального закона «О противодействии терроризму». В данном определении зафиксированы, по сути, два значения понятия терроризма: терроризм как идеология и терроризм как совокупность деяний. Однако далее в тексте Федерального закона эти значения никак не разграничиваются. Более того, определение одного из значений понятия терроризма идеологии насилия, связанного с устрашением населения и иными формам противоправных насильственных действий, представляется нетерпимо аморфным, поскольку под это определение подпадает понятие идеологии любой формы насильственной преступности. Стоит сразу подчеркнуть, что идеология насилия неразрывна с практикой воздействия на власть, и это деяние должно быть связано с устрашением населения и (или) иными формами противоправных насильственных действий (насилия). Сама по себе идеология насилия, даже приведшая к устрашению населения разновидностью терроризма признаваться не должна. Этот вывод подтверждается неоправданным, на наш взгляд, отождествлением террористических и экстремистских организаций в статье 24 Федерального закона «О

угроз на Северном Кавказе // Российская газета от 20 августа 2009 года. С.2.

[1] См.: С.В. Максимов. Эффективность общего предупреждения преступлений. – М.: Академия МВД РФ, 1992. С.6 – 20.

[2] См.: Ленин В.И. Полн. собр. соч., т. 39, с. 355.

[3] См.: СУ РСФСР, 1920, № 4 - 5. Там же, № 43.

противодействии терроризму»;

2. Неразработанность системы мер профилактики терроризма. В новом законе дается лишь определение понятия профилактики терроризма (ет,3). Однако сами меры профилактики терроризма остаются за пределами правового регулирования. В частности, никак не регламентируются мониторинг (анализ, оценка и прогноз) терроризма и отдельных его проявлений, их причин и условий, мер борьбы с ними; стандарты антитеррористического воспитания и антитеррористической пропаганды; планирование борьбы с терроризмом, в том числе и на территории СНГ.

3. Неоправданное «вторжение» в сферы регулирования, относящиеся к другим отраслям права. Например, в статье 22 рассматриваемого Федерального закона закреплена частная уголовно-правовая норма, противоречащая к тому же общим уголовно-правовым нормам, регламентирующим обстоятельства, исключающие преступность деяния (ст. 37-42 УК РФ).

К другим несовершенствам нового антитеррористического законодательства мы можем отнести, в частности следующее: из части содержания ч.2 статьи 16 данного Федерального закона вытекает, что при ведении переговоров с террористами в ходе террористической операции не должны рассматриваться выдвигаемые ими политические требования. При этом ни понятие «террорист», ни понятие «политические требования» в Законе не определены, что на наш взгляд, обессмысливает данную норму.

Новый антитеррористический закон России обладает большим числом юридико-технических недостатков, некоторые из которых требуют немедленного исправления. Так, в соответствии с п.1 ч.1 ст. 10 этого закона для пресечения международной террористической деятельности допускается применение вооружения с территории Российской Федерации против находящихся за ее пределами террористов и (или) их баз. Данное положение, на наш взгляд, не подлежит применению до тех пор, пока в Уголовном кодексе РФ, данном или ином Федеральном законе не будут определены понятия «международная террористическая деятельность», «террорист» и «база террористов». Исходить из правила, согласно которому, соответствующие понятия будут определены в международном договоре Российской Федерации и станут применяться с момента его ратификации, на наш взгляд, нельзя. В частности, потому что часть названных положений носит специфический уголовно-правовой характер. Согласно п.6 Постановления №5 Пленума Верховного суда Российской Федерации «О применении судами общей юрисдикции общепризнанных принципов и норм международного права и международных договоров Российской Федерации» от 10 октября 2003 г. «Международные договоры, нормы которых предусматривают признаки составов уголовно-наказуемых деяний, не могут применяться судами непосредственно, поскольку такими договорами прямо устанавливается обязанность государств обеспечить выполнение предусмотренных договором обязательств путем установления наказуемости определенных преступлений внутренним (национальным) законом».

Установленные в статье 22 рассматриваемого Федерального закона правила правомерного причинения вреда лицу, совершающему террористический акт, противоречат многочисленным оговоркам, содержащимся в ст. 37-42 УК, и потому не подлежат применению до внесения соответствующих изменений в УК РФ или в рассматриваемый Федеральный закон. Например, предусмотренная ст.38 УК оговорка, согласно которой причинение вреда при задержании лица, совершившего преступление возможно лишь в том случае, если иными средствами задержать такое лицо не представлялось возможным, не позволяет считать правомерным любое лишение жизни террориста при его задержании Российское государство на современном этапе развития противопоставляет различным проявлениям вооруженного сепаратизма, экстремизма и терроризма сложный социально-политический механизм борьбы, подчиненный общей цели - обеспечению эффективной борьбы с преступностью данного вида с наименьшими затратами и издержками.

Название принятого 6 марта 2006 гада закона «О противодействии терроризму» концептуально отличается от прежнего, утратившего силу закона «О борьбе с терроризмом». Термины борьба и противодействие по содержательному объему не равнозначны. Они находятся в соотношении соподчинения как часть и целое. Противодействие это более широкий спектр деятельности, на котором должны объединятся усилия всех государственных и общественных институтов, ориентированных на выявление причин и условий совершения террористических преступлений, а также и на борьбу с ними. Такая концепция нашла отражение и в ФЗ «О противодействии экстремистской деятельности» 2002 года (и в названии и в тексте). Это находит подтверждение в системе принципов противодействия терроризму, закрепленных в ст.2 ФЗ от 6 марта 2006 года. В сравнении с Федеральным зерном «О борьбе с терроризмом» их стало больше - 13, вместо 9. И «старые» и те, что добавились (а 9 из них идентичны или почти повторяют формулировку ст.2 ФЗ от 26 июля 1998 года) как раз и отражают основную направленность Закона.

Кардинально обновлен понятийный аппарат законодательного акта. Основной дефиницией формулирующей явление (деяние, поведение), на которое следует воздействовать, является «терроризм». Под ним в законе понимается «идеология насилия и практика воздействия на принятие решения органами государственной власти, органами местного самоуправления или международными организациями, связанные с устрашением населения и (или) иными формами противоправных насильственных действий».

ОРГАНИЗАЦИОННО-ПРАВОВЫЕ ПРОБЛЕМЫ ИНФОРМАЦИОННОГО ОБЕСПЕЧЕНИЯ УПРАВЛЕНИЯ СИЛАМИ И СРЕДСТВАМИ ОВД ПРИ РЕЗКОМ ОСЛОЖНЕНИИ ОПЕРАТИВНОЙ ОБСТАНОВКИ.

В.А. Семенов (Академия управления МВД России)

При постоянном росте и усложнении задач, стоящих перед МВД России, происходящем на фоне сокращении штатного состава органов внутренних дел, а также из-за ряда объективных проблем, в первую очередь связанных с недостаточным материально-техническим и кадровым обеспечением, повышение результатов борьбы ОВД с противоправными проявлениями экстенсивными методами в значительной мере затруднено. Поэтому МВД России принимает меры по ослаблению негативного влияния имеющихся проблем на реализацию необходимых мероприятий путем повышения уровня организации управления и эффективности использования имеющихся сил и средств.

Одним из основных направлений решения указанных проблем является совершенствование информационного обеспечения органов внутренних дел на основе оснащения их современными аппаратно-программными комплексами и системами, а также внедрение в практическую деятельность новых и перспективных информационных технологий. Сложность проведения мероприятий по противодействию угрозам осложнения оперативной обстановки заключается в необходимости проведения целого комплекса мер, в том числе воздействия на факторы, способствующие их возникновению и развитию (экономические, культурные и социальные), а также в особенностях применяемых преступниками методов и средств, в том числе применении высоких технологий, фактора внезапности и других[1].

Качественное решение вопросов повышения эффективности работы органов внутренних дел на основе более полного и детального раскрытия резервов управления и его центрального элемента - управленческой деятельности - требуют дальнейшего исследования перспективы совершенствования организационной составляющей. Совершенствование системы управления в современных условиях невозможно без использования современных информационных технологий, поскольку именно вопросы обработки информации являются на сегодняшний день критическими[2].

С 2005 года в рамках Федеральной целевой программы «Электронная Россия» проводятся мероприятия по созданию Единой информационно-телекоммуникационной системы МВД России[3]. Формирование современной информационно-телекоммуникационной инфраструктуры информационного обеспечения органов внутренних дел для обеспечения технической возможности повышения эффективности деятельности правоохранительных органов по защите прав и свобод граждан, обеспечения законности, правопорядка и общественной безопасности путем реконструкции и оборудования объектов органов внутренних дел новыми и перспективными телекоммуникационными и программно-техническими комплексами с использованием современных телекоммуникационных, информационных и биометрических технологий явилось бы мощным инструментом по противодействию противоправным проявлениям.

Сеть подключенных к ЕИТКС пользователей последовательно расширяется, так, на 01.07.2009 г. в органах внутренних дел УВД по Оренбургской области в общую систему организован вход с 2042 рабочих мест, общее количество запросов к информационной базе данных ИБД-«Регион» составило 1006602, что на 5,8 % больше, чем за аналогичный период прошлого года, с помощью автоматизированной дактилоскопической информационной системы АДИС «Папилон» получено положительных идентификаций по 407 уголовным делам, всего с помощью ресурсов системы за 6 месяцев текущего года раскрыто 11179 преступлений.

Вместе с тем, анализ результатов внедрения ЕИТКС показал, что из-за отсутствия строгой правовой и организационной регламентации большинство имеющихся автоматизированных информационных систем характеризуются отсутствием унифицированного программного обеспечения и наличием существенных функциональных ограничений, не позволяющих использовать современные информационные технологии для выполнения качественного анализа информации при осложнении оперативной обстановки. Руководство МВД России отмечает, в частности, что в ходе внедрения ЕИТКС не решены или решены не в полном объеме вопросы:

- создания базовой технической инфраструктуры единого информационного пространства МВД и ВВ России и обеспечения взаимодействия между существующими специализированных территориально-распределенных автоматизированных систем;
- создания современных систем передачи информации ограниченного доступа и информации, содержащей сведения, составляющие государственную тайну; …
- развития в полном объеме банков данных биометрической и розыскной информации;
- автоматизации картотек[4].

В связи с этим необходимо при разработке нормативно-правовых актов, регулирующей деятельность ОВД и ВВ в области информатизации, учитывать особенности функционирования правоохранительных

[1] Приказ МВД России от 20 мая 2008 г. № 435 «Об утверждении новой редакции программы МВД России «Создание Единой информационно-телекоммуникационной системы органов внутренних дел»»

[2] Отчет о НИР по теме: «Совершенствование системы оперативного управления ОВД Российской Федерации в повседневных и особых условиях службы на основе современных информационных технологий», Академия управления МВД России, 2008 г.

[3] В дальнейшем «ЕИТКС»

[4] Приказ МВД России от 4 апреля 2009 г. № 280 «Об утверждении Концепции информатизации органов внутренних дел Российской Федерации и внутренних войск МВД России до 2012 года»

органов при резком обострении оперативной обстановки, на постоянной основе привлекать практических специалистов для оценки эффективности мероприятий по совершенствованию информационной системы.

ПСИХОЛОГИЧЕСКОЕ ОБЕСПЕЧЕНИЕ УПРАВЛЕНИЯ ОРГАНАМИ ВНУТРЕННИХ ДЕЛ ПРИ ПРОВЕДЕНИИ КОНТРТЕРРОРИСТИЧЕСКИХ МЕРОПРИЯТИЙ

В.Н Смирнов (Академия управления МВД России)

Терроризм в любых формах проявления угрожает безопасности многих стран и их граждан, влечет за собой весьма существенные политические, экономические потери, оказывает сильное психологическое воздействие на большие массы людей, уносит жизни мирных жителей. Деятельность террористических организаций нацелена не просто на обострение и дестабилизацию обстановки в том или ином районе во имя решения каких-либо задач, а захват или передел власти, территориальный передел, насильственное изменение конституционного строя в тех или иных странах[1].

Основными социальными корнями и предпосылками роста терроризма на международном уровне по мнению многих исследователей являются[2:]

вступление общества на путь трансформаций, резких социальных изменений или современные постмодернизированные общества с выраженной поляризацией населения по этносоциальным признакам. Участниками террористических действий становятся маргинальные и иммобильные группы населения;

резкое расслоение общества на бедных и богатых, социальные контрасты, а не просто бедность или низкий уровень социально-экономического статуса, провоцируют агрессию и создают почву для терроризма;

социальные модернизации общества провоцируют проявления экстремизма, особенно в начальные периоды реформ. Изменения этнодемографической структуры общества, особенно нерегулируемая миграция, также порождают экстремизм и интолерантность в обществе;

преобладание авторитарных политических режимов в исламском мире играет важную роль в распространении этнического и религиозного экстремизма и терроризма. Эти режимы провоцируют насилие при разрешении политических противоречий и придают ему характер культурной нормы.

Что касается современного состояния российского общества наиболее типичными, порождающими терроризм причины, в концентрированном виде являются следующие:

- отсутствие общепринятой стратегии развития общества, принимаемые концепции зачастую не согласуются с желаниями общества;
- углубляющиеся противоречия в сфере экономики, обусловленные проблемами построения рыночной экономики, отсутствием надежных ее механизмов, неприятием частью населения новых экономических отношений и методов перехода к ней;
- растущая социальная дифференциация, дальнейшее расслоение общества на богатых и бедных, неуверенность в завтрашнем дне, отсутствие «социума благополучия и выживания»;
- низкая эффективность функционирования системы власти, государственного аппарата и правоохранительных структур, отсутствие эффективных инструментов и средств правовой защиты населения, особенно в кризисных ситуациях;
- обострение и дальнейшее углубление «грязных технологий» в борьбе за власть политических партий, движений, общественных объединений, преследующих политические цели, либо отдельных групп, лидеры которых преследуют собственные цели, вплоть до устранения конкурентов различными методами;
- отсутствие современных и эффективных защитных институтов, функционирующих в сфере нравственности и морали; утрата общечеловеческих установок, мотиваций и ценностей в воспитательной работе, особенно в молодежной среде;
- жесткое, целенаправленное воздействие и распространение «западной культуры и мифов», формирующих жестокость и вандализм в отношении другой личности и человеческого поведения, общежития и порождающих «фанатизм» в субкультуре поведения;
- нарастающие тенденции разрешения возникших противоречий, конфликтов и кризисных ситуаций силовыми способами и методами, вызывающими неадекватную оценку общества и общественный резонанс, выходящий за пределы как отдельной территории, так и государства;
- углубление социальных противоречий под влиянием растущей преступности, особенно организованной, вырабатывающей и использующей современные информационные технологии и системы «защиты» на всех уровнях, постоянное обновление и пополнение криминала из числа законопослушных граждан, оказавшихся в безысходном материальном положении и используемых, как правило, для совершения разовых акций (за определенную сумму перевезти взрывоопасные вещества либо оставить в условленном месте);
- неразрешенные противоречия либо отсутствие отдельных законодательных актов, четко определяющих как общеправовые, так и уголовно-правовые механизмы мер борьбы с терроризмом.

---

[1] Ольшанский Д.В. Психология терроризма. СПб. 2002. Решетников М.М, Психология и психопатология терроризма. Гуманитарные стратегии антитеррора – СПб.: Восточно-Европейский Институт Психоанализа, 2004.

[2] Дробижева Л., Паин Э. Политический экстремизм и терроризм: социальные корни проблемы // Век толерантности / Под ред. А. Асмолова. М., 2003. Вып. 5. Психологи о терроризме// Психологический журнал. Т.16.,1995.№4

В соответствии с указанными причинами для руководителей органов внутренних дел актуальной задачей является изучение основ психологического обеспечения антитеррористической деятельности, организации работы с населением, подвергшимся террористической атаке, оказания психологической помощи пострадавшим.

Психологическое обеспечение управления органами внутренних дел участвующих в проведении контртеррористических операций, раскрытия и расследования террористических актов осуществляют сводные группы психологов, сформированных из числа наиболее опытных и квалифицированных специалистов и психологи оперативных подразделений. Задачами психологической службы МВД России по указанному направлению являются:

1. Психологическое обеспечение управления оперативно-служебной деятельностью, включающее участие в консультировании переговорщиков по ведению переговоров при освобождении заложников, составление психологических портретов предполагаемых преступников; проведение консультаций, разработку рекомендаций руководителям по моделированию и проведению оперативных комбинаций, привлечению лиц к негласному сотрудничеству; по организации и проведению профессионально-психологической подготовки, сопровождению разведчиков в процессе их деятельности по выявлению и разоблачению террористических групп; по психологическому анализу поступающей оперативной информации и выработке на его основе рекомендаций по упреждающим оперативно-следственным действиям.

2. Оказание психологической помощи руководителям при организации ими мероприятий направленных на восстановление работоспособности личного состава (психологическая реабилитация, психологическое восстановление, поддержание психологической устойчивости) и поддержание благоприятного психологического климата в подразделениях (консультации по социально-психологическим вопросам) в процессе и после проведения контртеррористических мероприятий.

3. Разработка предложений руководителям подразделений и служб органов внутренних дел по взаимодействию со средствами массовой информации при подготовке и проведении контртеррористических операций; участие в подготовке проектов обращений руководителей органов внутренних дел к населению; анализ содержания публикаций и информационных передач, выявление возможных непосредственных и отдаленных негативных социально-психологических последствий негативного информационного воздействия и выработка на основе полученных выводов практических рекомендаций руководителям.

Результаты деятельности психологической службы системы МВД России свидетельствует о том, что решение организационных и методических вопросов психологического обеспечения управления органами внутренних дел при совершении террористических актов приобретает все большее признание среди руководителей органов внутренних дел. Это позволяет психологам принимать активное участие в планировании оперативных мероприятий антитеррористической направленности, в контртеррористических операциях, ликвидации последствий террористических актов, проведении первоочередных мероприятий по оказанию психологической помощи пострадавшим, сопровождении деятельности сотрудников, принимающих участие в ликвидации последствий террористических актов.

При планировании и проведении оперативно-розыскных мероприятий антитеррористической направленности психологи оперативных подразделений помогают руководителям в своевременной дифференциации большого объема разнообразной, часто противоречивой и неполной информации (заявлений, писем, сводок, сообщений, информации личного сыска, информации полученной из конфиденциальных источников). Часто среди этого потока информации встречается специально «подбрасываемая» дезинформация. Такая информация должна вычленяться и на ее основе готовятся рекомендации по активному или пассивному противодействию.

Оперативные психологи помогают руководителям готовить оперативные комбинации направленные на противодействие готовящихся провокаций со стороны террористических групп, соблюдая при этом элементы конспирации для достижения позитивных результатов в будущих уже запланированных оперативно-следственных мероприятиях нацеленных на полное разоблачение и документирование преступников. Они оказывают существенную помощь руководителям в разработке оперативных комбинаций по внедрению разведчиков в организованные преступные группы террористической направленности или имеющих непосредственный контакт с этими организациями.

Существенна помощь психологов руководителям органов внутренних дел в осуществлении ими профессионального общения с личным составом, с населением, конфидентами, свидетелями, подозреваемыми, террористами.

По многочисленным данным руководителей ОВД, использующих помощь психологов для работы с личным составом в условиях проведения контртеррористических мероприятий, отмечают ее высокую эффективность и полезность. Достоинства психологических методов заключаются в том, что они предоставляют сотрудникам возможность мобилизации собственных ресурсов для преодоления стресса; позволяют лучше понять природу травматического стресса, его проявления и способы преодоления с тем, чтобы использовать эти знания при возможных новых драматических случаях.

Таким образом, система психологического обеспечения играет существенную роль в повышении эффективности управления органами внутренних дел при осуществлении сотрудниками ОВД контртеррористической деятельности, раскрытии и расследования преступлений террористической направленности.

ОРГАНИЗАЦИОННОЕ И ИНФОРМАЦИОННоЕ ОБЕСПЕЧЕНИЕ ДЕЯТЕЛЬНОСТИ ОРГАНОВ ВНУТРЕННИХ ДЕЛ РЕСПУБЛИКИ КАРЕЛИЯ ПО ПРЕДУПРЕЖДЕНИЮ И ПРЕСЕЧЕНИЮ ПРЕСТУПЛЕНИЙ ТЕРРОРИСТИЧЕСКОЙ И ЭКСТРЕМИСТКОЙ НАПРАВЛЕННОСТИ

С.В.Киселев (МВД по Республике Карелия)

В Указе Президента Российской Федерации Д.А. Медведева от 12.05.2009 №537 «О Стратегии национальной безопасности Российской Федерации до 2020 года» отмечается:

«Российская Федерация при обеспечении национальной безопасности в сфере государственной и общественной безопасности на долгосрочную перспективу исходит из необходимости постоянного совершенствования правоохранительных мер по выявлению, предупреждению, пресечению и раскрытию актов терроризма, экстремизма, других преступных посягательств на права и свободы человека и гражданина, собственность, общественный порядок и общественную безопасность, конституционный строй Российской Федерации».1

Поэтому одной из важнейших задач, стоящих в настоящее время перед органами внутренних дел страны, является обеспечение правопорядка и безопасности населения в условиях террористической и экстремисткой угрозы.

В органах внутренних дел Республики Карелия накоплен значительный опыт организации информационного обеспечения и контроля за оперативной обстановкой.

Автоматизированная информационная система «Оперативная обстановка», предназначенная для учета всех зарегистрированных на территориях обслуживания ОВД Карелии сообщений о преступлениях и иной информации о правонарушениях, помимо формирования ежесуточных сводок о зарегистрированных преступлениях и происшествиях в каждом ГО-РОВД и в целом по республике позволяет осуществлять контроль за разрешением всех зарегистрированных заявлений, сообщений и иной информации на уровне ГО-РОВД и особо значимых преступлениях на уровне МВД по Республике Карелия, формировать статистические сведения о складывающейся оперативной обстановке в целом по республике, в разрезе районов и городов за сутки, неделю, месяц и т.д., анализировать результаты работы различных служб по выявлению и раскрытию преступлений, эффективности работы СОГ на местах происшествий, проведения специальных операций и т.п.

Результаты работы органов и подразделений МВД по Республике Карелия за истекшие сутки ежедневно рассматриваются на рабочих совещаниях у министра внутренних дел по Республике Карелия с участием руководителей служб и отчетами дежурной части и ответственных руководителей о проделанной работе.

Сведения, содержащиеся в различных отчетах, накапливаются в информационно-аналитической системе «Регион», предназначенной для формирования информационно-аналитических материалов о состоянии преступности на территориях обслуживания и результатах работы органов, подразделений и служб за различные периоды отчетности в разрезе горрайорганах и республики в целом в сравнении с самими собой, а также в сравнении с аналогичными показателями субъектов России в Северо-Западном Федеральном округе и Российской Федерации в целом.

Доступ к базе данных системы «Регион» имеют пользователи локально-вычислительной сети аппарата МВД по Республике Карелия, а также горрайорганы в режиме удаленного доступа по выделенным и коммутируемым каналам связи. Это позволяет руководителям различного уровня оперировать едиными данными, в основе которых формируемые Информационным центром государственные, ведомственные и местные отчеты, а также предоставляемые ГИАЦ МВД России обобщенные данные в целом по стране и по федеральному округу. Другие сведения, например формируемые службами или горрайорганами по своей инициативе, руководством МВД по Республике Карелия к рассмотрению не принимаются.

В настоящее время в МВД по Республике Карелия продолжаются работы по комплексному развитию и широкому внедрению в практическую деятельность республиканского сегмента ЕИТКС МВД РФ. Это позволит в полной мере минимизировать информационные потоки по сбору данных и повысить качество и эффективность информационного обеспечения повседневной деятельности органов внутренних дел Карелии на основе современных безбумажных технологий.

По инициативе органов внутренних дел активно внедряются системы видеонаблюдения и экстренного вызова милиции на улицах, площадях, местах массового пребывания граждан и других общественных местах в рамках АПК «Безопасный город».

Решением Антитеррористической Комиссии в Республике Карелия из числа сотрудников различных министерств, ведомств и предприятий были созданы 7 рабочих групп Антитеррористической комиссии по различным направлениям, в том числе рабочая группа по вопросам противодействия терроризму на объектах проживания и массового пребывания граждан, возглавляемая министром внутренних дел по Республике Карелия.

Планирование работы группы осуществляется в соответствии с решениями Антитеррористической комиссии в Республике Карелия. Рабочая группа является постоянно действующим органом

[1] "Российская газета", N 88, 19.05.2009

Антитеррористической комиссии в Республике Карелия и выполняет задачи по:

- координации деятельности федеральных и республиканских органов исполнительной власти по противодействию терроризму в местах проживания и массового пребывания граждан;
- подготовке материалов к заседаниям Антитеррористической комиссии в Республике Карелия в соответствии с планом ее работы;
- проведению анализа состояния антитеррористической защищенности на объектах проживания и массового пребывания граждан;
- разработке предложений по усилению антитеррористической защищенности объектов проживания и массового пребывания граждан, профилактике и минимизации последствий террористических актов (с этой целью организуются проверки объектов).

В состав группы включены сотрудники подразделений МВД по Республике Карелия и согласованные с членами Антитеррористической комиссии в Республике Карелия представители федеральных и республиканских органов исполнительной власти, эксперты. Состав рабочей группы утверждается руководителем группы и уточняется ежегодно с информированием аппарата Комиссии. Исходя из оперативной обстановки и реальной потребности, состав группы может быть увеличен по решению руководителя группы.

Работа группы осуществляется на плановой основе. План работы группы, как правило, на год, утверждается руководителем группы. Заседания группы проводятся ежеквартально. Копия протокола заседания группы направляется в аппарат Комиссии. По результатам работы за год руководитель группы информирует аппарат Комиссии.

Члены группы в работе руководствуются действующим законодательством РФ, ведомственными нормативными правовыми актами по направлению деятельности, решениями Антитеррористического комитета Российской Федерации и Антитеррористической комиссии в Республике Карелия, а также Положением о рабочей группе по противодействию терроризму в местах проживания и массового пребывания граждан Антитеррористической комиссии в Республике Карелия.

МВД по Республике Карелия совместно с другими правоохранительными органами проводит комплекс оперативно-профилактических мероприятий, направленных на недопущение распространения различного вида экстремизма.

В целях усиления профилактической работы в апреле текущего года разработаны графики проведения профилактических бесед в образовательных учреждениях.

На постоянной основе проводятся профилактические беседы с лидерами и активными участниками неформальных молодежных объединений.

Проводятся встречи с руководством высших и средних образовательных учреждений.

Подразделениями по борьбе с экономическими и налоговыми преступлениями МВД по Республике Карелия проводится работа по установлению фактов и каналов возможного финансирования деятельности молодежных, религиозных и иных неформальных организаций террористической и экстремистской направленности.

В целях взаимодействия с органами местного самоуправления и проверки организации работы по противодействию экстремизму и терроризму в горрайорганах республики осуществляются выезды в служебные командировки, в ходе которых состоялись встречи с сотрудниками администраций местного самоуправления.

Взаимодействие с органами государственной власти, правоохранительными органами осуществляется на постоянной основе, в т.ч. в рамках реализации Плана совместных мероприятий по противодействию экстремизму в молодежной среде, Плана согласованных действий органов исполнительной власти Республики Карелия, территориальных органов федеральных органов исполнительной власти в Республике Карелия, органов местного самоуправления муниципальных образований Республики Карелия по реализации Стратегии профилактики экстремизма в Республике Карелия.

Проводится взаимное информирование о проблемных вопросах в сфере профилактики и борьбы с экстремизмом и терроризмом.

15 апреля 2009 г. с участием сотрудников МВД по Республике Карелия состоялось заседание Общественного совета при Главе Республики Карелия по профилактике экстремистской деятельности на тему: «О мерах, направленных на повышение уровня взаимодействия со средствами массовой информации по вопросам профилактики экстремизма». Принято решение о развитии практики проведения фестивалей и конкурсов телерадиопрограмм и изданий, создающих произведения, направленные на профилактику экстремизма в обществе.

Сотрудниками ОИОС МВД по Республике Карелия подготовлен материал «Работа с молодежью сегодня – общество без экстремизма завтра».

В материале дана характеристика межнациональных отношений в республике, охарактеризована работа республиканских органов власти и правоохранительных структур. Приведены данные социологического исследования «Особенности межнациональных и межрелигиозных отношений в Республике Карелия». Также данный материал был размещен на нескольких интернет-сайтах.

Таким образом, органами государственной власти и правоохранительными органами в целом обеспечен контроль за нераспространением проявлений экстремизма на территории республики.

Для закрепления достигнутого результата следует продолжить проведение профилактической работы по различным направлениям деятельности. В период летних школьных и студенческих каникул возможно

проведение на территории республики летних лагерей, организуемых организациями «различного толка», поэтому разрешение подобных мероприятий должно приниматься органами власти с учетом мнения правоохранительных органов. Именно в данный период необходимо качественно организовать летний отдых детей с целью недопущения вовлечения их в различные антиобщественные группы и движения.

Важнейшей организационной основой взаимодействия органов государственной власти республики, органов местного самоуправления и правоохранительных органов являются республиканская и районные (городские) программы профилактики и борьбы с преступностью, в которых важнейшее место отводится, прежде всего, мероприятиям, направленным на укрепление антитеррористической защиты населения и профилактики экстремисткой.

Нами извлечен серьезный урок из событий в сентябре 2006 г. в г. Кондопога, где произошли массовые беспорядки вследствие возникшего конфликта между группой местных жителей и выходцами с Кавказского региона. Данный инцидент имел большой общественный резонанс. Детально изучены причины, которые привели к таким трагическим последствиям, дана принципиальная оценка действиям сотрудников милиции. Сделанные выводы свидетельствуют о том, что крайне необходимо совершенствовать навыки органов внутренних дел по действиям при возможном возникновении массовых беспорядков.

Одним из основных условий достижения успеха в выполнении задач при чрезвычайных обстоятельствах является подготовка сил и средств к действиям при чрезвычайных обстоятельствах (ЧО). Цель данной подготовки - обеспечение слаженных действий органов управления, группировки сил и средств при ЧО. Мы провели подготовку сотрудников милиции для действий при возникновении чрезвычайных обстоятельств, разработали учебно-методические материалы МВД по Республике Карелия - «Организация планирования и управления органами внутренних дел при подготовке и в ходе действий при возникновении чрезвычайных обстоятельств», «Тактика действий ОВД при проведении операций в условиях чрезвычайных обстоятельств и ситуаций», которые направлены во все ГО-РОВД для изучения, использования в служебной деятельности и совершенствования подготовки органов управления и элементов группировки сил и средств ОВД республики к действиям при чрезвычайных обстоятельствах.

В целях совершенствования порядка и содержания подготовки органов внутренних дел республики к выполнению задач при возникновении чрезвычайных обстоятельств, заблаговременной подготовки сил и средств в интересах обеспечения их высокой оперативно-служебной и служебно-боевой готовности к действиям в экстремальных условиях МВД по Республике Карелия регулярно проводит тактико-специальные учения, командно-штабные учения, штабные тренировки, тактико-специальные занятия и тренировки, в ходе которых совершенствуются навыки руководителей оперативных штабов по организации управления силами и средствами органов внутренних дел, принятию управленческих решений, совершенствуются устойчивые морально-психологические качества у обучаемых при резком осложнении оперативной обстановки на территории обслуживания, с практической отработкой тактики действий элементов группировки сил и средств непосредственно на местности, для чего создается сложная динамическая обстановка.

МВД по Республике Карелия в соответствии с планами антитеррористических учений, утвержденными председателем национального антитеррористического комитета, активно принимает участие в подготовке и проведении тактико-специальных учений, командно-штабных учений, командно-штабных тренировок, в ходе которых отрабатывается взаимодействие между территориальными органами исполнительной власти, входящими в оперативный штаб в Республике Карелия при проведении контртеррористических операций.

Проведение учений позволяет поддерживать готовность МВД по Республике Карелия к действиям в экстремальных условиях на высоком уровне.

Актуальной задачей общепрофилактической деятельности органов внутренних дел является восстановление общественных формирований правоохранительной направленности, укрепление связи с населением. Необходимо более активно организовывать выступления работников милиции, прежде всего участковых уполномоченных, по вопросам борьбы с преступностью и охраны общественного порядка перед населением.

Правовой основой добровольного участия жителей Республики Карелия в охране общественного порядка является Закон Республики Карелия «Об участии жителей Республики Карелия в охране общественного порядка», принятый Законодательным Собранием Республики Карелия 24 февраля 2005 года.

Данный закон определил формы такого участия в целях укрепления взаимодействия жителей Республики Карелия с правоохранительными органами и органами местного самоуправления. Участие граждан в охране общественного порядка может быть индивидуальным (пропаганда правовых знаний; содействие правоохранительным органам в профилактической работе с лицами, склонными к совершению правонарушений; содействие органам и учреждениям системы профилактики безнадзорности и правонарушений несовершеннолетних; иные не запрещенные законодательством формы участия в охране общественного порядка) и коллективным (членство или участие в общественных объединениях, созданных и действующих в порядке, установленном Федеральным законом от 19 мая 1995 года N 82-ФЗ "Об общественных объединениях", и уставные цели которых предусматривают оказание содействия правоохранительным органам; участие в работе народной дружины муниципального образования).

Однако, как представляется, требуется скорейшее принятие и закона на федеральном уровне.

Как показывает практический опыт работы органов внутренних дел Республики Карелия, следует внести изменения в уголовное законодательство, усиливающие ответственность за должностные преступления,

терроризм, преступления, связанные с незаконным оборотом оружия, сбытом взрывчатых веществ и изготовлением взрывных устройств, разжигание национальной, религиозной и расовой розни, незаконный оборот наркотических средств.

Данные предложения, безусловно, не исчерпывают всего круга вопросов данной темы. Тем не менее, их решение, как показывает опыт, будет способствовать активизации борьбы с терроризмом и экстремизмом.

РЕГИОНАЛЬНЫЕ АСПЕКТЫ ПРОТИВОДЕЙСТВИЯ РАСПРОСТРАНЕНИЮ ЭКСТРЕМИЗМА (НА ПРИМЕРЕ УДМУРТСКОЙ РЕСПУБЛИКИ)

С.Г. Поволоцкий (МВД по Удмуртской Республике)

Экстремизм и терроризм сегодня превратились в серьезнейшие проблемы, с которыми человечество вошло в XXI столетие. Терроризм и экстремизм в любых формах их проявления все больше угрожают безопасности многих стран и их граждан, влекут за собой существенные политические, экономические и моральные потери, оказывают сильное психологическое воздействие на большие массы населения, уносят жизни ни в чем не повинных людей.

Международный терроризм и экстремизм сегодня не признают ни религиозных, ни национальных, ни государственных границ. Этому способствуют ослабление административно-правовых режимов, нерешенность социальных, национальных, религиозных и иных проблем, другие факторы, нуждающиеся в самостоятельном анализе. Внутренние причины этих преступлений часто бывают связаны с борьбой за политическую власть, передел собственности, с мафиозной активностью, с межэтническими и межрелигиозными конфликтами.

В своем ежегодном Послании Федеральному собранию Российской Федерации Президент Российской Федерации определил рост экстремизма как «серьезную угрозу стабильности и общественной безопасности». Одновременно он обоснованно отметил, что «милиция и прокуратура часто не имеют достаточно эффективных инструментов для привлечения к ответственности организаторов и вдохновителей» преступлений экстремистской направленности.

Федеральный закон от 25 июля 2002 г. № 114-ФЗ «О противодействии экстремистской деятельности» закрепляет за органами внутренних дел конкретные задачи в сфере противодействия экстремизму. Статья 4 названного Закона дает достаточно широкое понятие субъектов противодействия экстремистской деятельности, а также сферы их деятельности. В соответствии с этой нормой федеральные органы государственной власти, органы государственной власти субъектов Российской Федерации, органы местного самоуправления участвуют в противодействии экстремистской деятельности «в пределах своей компетенции».

Анализируя сложившуюся обстановку, можно сделать вывод, что борьба с преступлениями террористического характера и экстремистской направленности становится одной из важнейших задач сотрудников органов внутренних дел. В полной мере это относится и к сотрудникам МВД по Удмуртской Республике[1].

В целом, комплекс мероприятий МВД по линии противодействия терроризму и экстремизму осуществляется по следующим основным направлениям:

пресечение противоправной деятельности представителей этнических объединений и борьба с нелегальной миграцией;

противодействие проявлениям экстремизма в религиозной среде;

пресечение каналов финансирования террористических, экстремистских организаций;

противодействие проявлениям экстремизма в молодежной среде;

осуществление профилактических мероприятий по недопущению террористических и экстремистских акций.

По национальному составу Удмуртия относится к разряду наиболее многонациональных субъектов Российской Федерации, на территории которой проживают представители более ста национальностей, из них 60% населения составляют русские, 29,3% - удмурты, 7% - татары и 3,6% - другие национальности, в том числе выходцы из Северо – Кавказского региона и стран СНГ, которые объединены в группы по этническому признаку.

Всего сформировалось 6 устойчивых этнических диаспор и общин: чеченская, дагестанская, азербайджанская, армянская, таджикская и узбекская.

Интересы представителей указанных диаспор и общин представляют 7 официально зарегистрированных в Удмуртии этнических организаций (2 узбекские). Деятельность данных организаций направлена на налаживание тесных связей между местным населением республики и представителями этнических землячеств в социальной, экономической, культурной, религиозной и образовательной сферах.

Чеченская община.

Удмуртская республиканская общественная организация «Чеченский национально-культурный центр «Даймохк» (Родина). Местами компактного проживания являются: г.г. Ижевск, Воткинск, Глазов и Ярский район УР. Лица чеченской национальности на территории Удмуртии занимаются реализацией деловой древесины и мукомольной продукции, производством строительных работ.

Дагестанская община.

[1] Далее - МВД

Дагестанский общественный центр Удмуртии «Горец». Местом концентрации является г. Ижевск. Основное занятие лиц дагестанской национальности - продажа промышленных товаров, меховых изделий, поставка фруктов.

Азербайджанская диаспора.

Региональная общественная организация «Азербайджанский общественный центр Удмуртии «Достлуг». Места компактного проживания: гг. Ижевск, Воткинск, Глазов, Сарапул, а так же Завьяловский, Балезинский и Якшур-Бодьинский районы УР. Основная часть азербайджанцев имеет Российское гражданство, предпочитает заниматься коммерческой деятельностью, а именно, торговлей фруктами, цветами, продуктами питания.

Армянская диаспора.

Армянская общественная организация Удмуртской Республики «Урарту». Места компактного проживания: г.г. Ижевск, Сарапул, Глазов, а так же Завьяловский, Малопургинский и Ярский районы УР. Основной вид деятельности лиц армянской национальности на территории республики - предпринимательская деятельность в сфере торговли и оказания услуг.

Таджикская диаспора.

Республиканская общественная организация Таджикский общественный центр «Ориен-Тадж» (Благородные). Местами концентрации являются: г.г. Ижевск, Сарапул, Воткинск, Глазов, а так же Балезинский и Завьяловский районы УР. Основной вид деятельности представителей таджикской диаспоры - торгово-закупочная.

Узбекская диаспора.

Общественная организация «Узбекская национально-культурная община в Удмуртской Республике «Тинчлик» («Мир»);

Удмуртская Региональная общественная организация «Узбекский центр национальной культуры «Самарканд».

Местами компактного проживания являются г.г. Ижевск, Воткинск, Сарапул, Глазов, Можга, а так же Завьяловский, Балезинский, Малопургинский районы УР. Лица узбекской национальности, проживающие на территории республики, в большинстве своем, занимаются торгово-закупочной деятельностью.

Деятельность данных организаций направлена на налаживание тесных связей между местным населением республики и представителями этнических землячеств в социальной, экономической, культурной, религиозной и образовательной сферах.

Особое значение придается профилактической работе в этнической среде республики.

С целью предотвращения противоправных действий, а также недопущения сращивания с лицами, исповедующими радикальные течения ислама, на постоянной основе (еженедельно) проводятся разъяснительные беседы с представителями этнических объединений.

Принимаются меры по выявлению иностранных граждан, незаконно пребывающих и незаконно осуществляющих трудовую деятельность на территории республики. Работа в данном направлении осуществляется во взаимодействии с представителями УФМС России по УР.

С целью выявления нарушений миграционного законодательства за 2009 год было проведено 3483 профилактических мероприятия (АППГ – 3456, +0,8%). В результате проведенных мероприятий выявлены и привлечены к административной ответственности за нарушения законодательства в сфере миграции 4092 человека (АППГ – 4001, +2,3%), из них:

- 1913 иностранных граждан и лиц без гражданства привлечены по ст. 18.8 КоАП РФ за нарушение режима пребывания на территории Российской Федерации (АППГ - 1888, +1,3%);

- по ст. 18.9 КоАП РФ за нарушение правил пребывания иностранных граждан и лиц без гражданства в Российской Федерации привлечено 1522 человека (АППГ – 1386, +9,8%);

118 иностранных граждан и 135 граждан РФ по ст. 19.27 КоАП РФ за предоставление ложных сведений при осуществлении миграционного учета (АППГ – 75 и 124 соответственно, общий рост на 27,1%).

К административной ответственности за нарушения правил привлечения и использования иностранных работников выявлены и привлечены к административной ответственности:

271 иностранный работник по ст. 18.10 КоАП РФ за незаконное осуществление трудовой деятельности на территории РФ (АППГ – 390, -30,5%);

121 работодатель, нарушающий правила привлечения и использования иностранной рабочей силы по ст. 18.15 КоАП РФ (АППГ – 126, -4,0%).

11 правонарушителей по ст. 18.17 КоАП РФ за несоблюдение установленных в отношении иностранных граждан ограничений на осуществление отдельных видов деятельности (АППГ – 10, +10,0%).

В связи с проявлением кризисных явлений в экономике отмечается факт значительного сокращения приема на работу иностранных граждан из стран с визовым порядком въезда (дальнее зарубежье). За 2009 год оформлено 158 разрешений (АППГ – 996, снижение в 6,3 раза). Происходит сокращение объемов работ, соответственно, и сокращение привлечения иностранной рабочей силы. Работодателям выгоднее привлекать иностранных работников из стран ближнего зарубежья (в соответствии с действующим законодательством, данные работники оплачивают госпошлину за счет собственных средств, а не за счет работодателя).

В целом, анализ оперативной обстановки свидетельствует о том, что выходцы из республик Северного Кавказа и стран СНГ влияния на криминогенную обстановку в республике не оказывают. Проявления

межнациональной вражды отсутствуют.

Оперативная обстановка по линии религиозного экстремизма характеризуется следующими факторами.

На территории Удмуртской Республики религия представлена 21-й конфессией. Зарегистрировано 230 религиозных объединений различных конфессий, из них самые многочисленные: православные – 131, мусульманские – 20.

Интересы мусульманских объединений в Удмуртии представлены Региональным Духовным управлением мусульман республики. Руководство Муфтията располагается в Соборной мечети г. Ижевска Удмуртской Республики.

Религиозные объединения мусульман имеют 21 культовое здание, из них 18 мечетей и 3 молитвенных дома. Также, имеются молельные комнаты и мечеть в 4 - х исправительных учреждениях республики.

В настоящее время на территории Удмуртской Республики осуществляется подготовка к строительству культурного центра армянских общин Удмуртии.

Строительство других культовых учреждений на территории Удмуртской Республики на данный момент не планируется.

Проникновение идей радикального ислама на территорию республики возможно через лиц, прошедших обучение в религиозных мусульманских учреждениях – медресе, расположенных как на территории России, так и стран арабского пояса.

В ходе бесед с представителями Мусульманского Духовенства республики, установлено, что из числа жителей Удмуртии в зарубежных религиозных мусульманских учреждениях прошли обучение 15 человек. В настоящее время проходят обучение 46 человек, из них за рубежом - 5, на территории России - 41.

В ходе проведенных мероприятий установлено, что на обучение в религиозные мусульманские учреждения жители республики выезжают в частном порядке, при наличии достаточных финансовых средств. Действующие на территории республики мусульманские объединения направлением на обучение не занимаются. Централизованный учет лиц данной категории в Муфтияте республике не ведется. Проводится проверка данных лиц на возможную причастность к экстремистской деятельности.

С учетом этого сотрудниками МВД на постоянной основе проводятся профилактические беседы с представителями Муфтията республики. Ежемесячно осуществляется оперативно сопровождение «пятничных молитв», проходящих в Соборной мечети г. Ижевска.

Одними из носителей идей радикального ислама также могут являться лица, отбывающие наказание в исправительных учреждениях республики, осужденные за преступления террористического характера и экстремистской деятельности.

На сегодняшний день выявленные контакты свидетельствуют о том, что осужденные данной категории, в большинстве своем, поддерживают родственные связи.

К предупредительным мероприятиям относятся, в том числе перекрытие каналов нелегального поступления финансовых средств для обеспечения организованных преступных сообществ террористической направленности, которое включает в себя проверку крупных коммерческих, кредитно-финансовых учреждений и их связей с ОПС; выявление групп, сообществ, действующих в наиболее доходных отраслях экономики, экономических структур, связанных с террористами, наложение арестов на их счета и приостановление их деятельности.

При документировании преступной деятельности выходцев из Северо-Кавказского региона, Средней Азии и Ближнего Востока, проводится отработка версии об их причастности к финансированию НВФ и террористической деятельности.

В ходе проведения оперативно-розыскных мероприятий сотрудниками МВД выявлены факты должностного преступления со стороны муниципального служащего, которые выразились в проставлении печатей и отметок о прохождении медицинского осмотра в личные медицинские книжки выходцев из Узбекистана, без фактического проведения их медицинского осмотра и получении взятки за указанные действия. По данным фактам возбуждены уголовные дела.

Проведена отработка расположенных на территории оперативного обслуживания 25-х типографий, с руководством вышеуказанных организаций проведены профилактические беседы на предмет недопущения изготовления печатной продукции экстремисткой направленности.

В настоящее время продолжаются мероприятия по проверке финансово – хозяйственной деятельности коммерческих структур, имеющих связи с регионами Кавказа или возглавляемых лицами – выходцами из указанных регионов и возможно имеющих отношение к финансированию экстремистских и террористических формирований.

Продолжает оставаться актуальной проблема распространения экстремизма в молодежной среде.

Внедрение экстремизма в молодежную среду в настоящее время приобрело очень большие масштабы и имеет опасные последствия для будущего нашей страны, так как подрастающее поколение – это ресурс национальной безопасности, гарант поступательного развития общества и социальных инноваций. Молодежь в силу природных и социальных особенностей молодежного возраста способна не только адаптироваться, но и активно воздействовать на его позитивное изменение.

В момент значительных потрясений и переломов, периодически возникающих в процессе развития любого общества и связанных с существенными деформациями условий и образа жизни людей, внезапно образующимся вакуумом ценностей, изменением материальных показателей, неясностью жизненных

перспектив и неизбежным обострением противоречий, неформальные объединения становятся своего рода отдушиной для молодежи.

Неформальные молодежные группировки в большинстве своем немногочисленны, однако при проведении музыкальных, спортивных и т.п. мероприятий их численность резко возрастает. Состав их смешанный по возрасту и полу, большую часть составляют юноши.

Сегодня на оперативном учете МВД состоят 5 официально не зарегистрированных молодежных группировок радикального характера, общей численностью около 50 человек. Данные группировки условно можно разделить на две группы:

I. Националистического толка, идеология – «Россия для русских»;

1. Молодежная группировка «Неонацисты» (ранее ижевское отделение «Партии Свободы»),

2. Молодежная группировка «Другие» (бывшая «Стая») (считают себя патриотами, ранее выступали организаторами «Русского марша» в г. Ижевске),

II. Группировки «антифашистского» толка.

Указанные группировки («Автономное действие» и «Объединённый гражданский фронт») носят радикально - политический характер. Своей целью данные группировки считают – замену существующего правительства Удмуртской Республики.

3. Молодежная группировка «Автономное действие» (анархисты, забастовщики)

4. Молодежная группировка «Объединённый гражданский фронт» (забастовщики, участники протестных акций)

5. Молодежная группировка «Антифа» (оппоненты неонацистов)

В социальном плане участников указанных группировок можно охарактеризовать, что подавляющие их большинство проживает в неполных и малообеспеченных семьях.

Представители группировок антифашистского толка в основном обучаются в средне-технических и высших учебных заведениях. Участники указанных группировок, используя для прикрытия идеологию противодействия распространению фашизма, провоцируют конфликтные ситуации с представителями националистических группировок, а так же представителями различных группировок несовершеннолетних, сформированных по территориальному принципу (районы). В целях популяризации движения и избегания уголовной ответственности активно используют СМИ республики и Интернет. Всплеск активности пришелся на конец 2007, начало 2008 года. В настоящее время количество участников насчитывает около 30-40 человек. При необходимости могут собрать до 60 человек. Установлено, что представители движения «антифа» поддерживают отношения с единомышленниками из различных регионов страны: Кировская область, Пермский край, республики Татарстан.

Число участников всех указанных группировок не является постоянным. Печатные издания и «штаб – квартиры» отсутствуют.

Необходимо учитывать, что неформальные группировки в большей части представляют собой неконтролируемую молодежь, лишенную положительного влияния семьи, школы, рабочего коллектива, общественной организации, что является причиной совершения ими правонарушений и преступлений.

В прошедшем году за совершение общеуголовных преступлений и преступлений экстремисткой направленности задержаны несколько активных участников, в том числе лидеры молодежных группировок.

В январе 2009 года по факту вымогательства денежных средств под угрозой предмета используемого в качестве оружия (пневматический пистолет), возбуждено уголовное дело по статье 163 в отношении Фокеева А.Б., являющегося одним из лидеров неформальной молодежной группировки националистического толка «неонацисты». В настоящее время ФокеевА.Б. находится в следственном изоляторе (по ст.30, ч.2 ст.105 УК РФ).

В 2009 году за нанесение побоев и за совершение хулиганских действий на территории Октябрьского района города Ижевска задержано 8 участников неформальной молодежной группировки радикального толка «антифа», трое из которых в настоящее время привлекаются к уголовной ответственности.

За причинение тяжкого вреда здоровью в ходе массовой драки, имевшего место 23 сентября 2008г. в районе «речки Карлутки» арестован лидер неформальной молодежной группировки «неонацисты» Демин. Данное преступление имело большой общественный резонанс и находилось на контроле у руководства МВД и прокуратуры республики.

По факту совершения хулиганских действий в составе группы лиц по предварительному сговору, с применением предметов используемых в качестве оружия (ножи, бутылки), около магазина «Лукоморье» по ул. Советская г. Ижевска возбуждено уголовное дело по ч.2 ст. 213, в настоящее время к уголовной ответственности привлекаются 2 лидера и 1 активный участник группировки «антифа».

Также раскрыто уголовное дело (ранее было приостановлено за не установлением лица), возбужденное по факту нанесения побоев несовершеннолетней девушке в Первомайском районе. Задержан активный участник группировки «неонацисты» Криницин и в мае 2009 года осужден. Также в отношении Криницина возбуждено уголовное дело по ч. 1 ст. 223 и по ч. 1 ст. 222 УК РФ по факту изготовления и хранения взрывного устройства.

За истекший период 2010 года возбуждены и расследуются два уголовных дела по ст. 214 УК РФ в отношении Манаева А.В. учащегося ИжГТУ, по ст. 244 УК РФ в отношении Кассихина Н.А. учащегося Машиностроительного лицея №8 г. Ижевска.

В результате проведенных мероприятий установлено, что в республике в настоящее время предпринимаются попытки по становлению 2-х новых неформальных молодежных объединений радикального толка, это группировка «Смена» (идеология схожа с ранее действовавшей организацией «НБП») и движение «РКСМб». Во взаимодействии с сотрудниками ФСБ проводятся первоначальные проверочные мероприятия.

С целью противодействия возможного распространения экстремистской идеологии в учебных заведениях, расположенных на территории республики, сотрудниками МВД проводятся встречи с руководителями ВУЗов, направляются информационные письма проводятся профилактические мероприятия направленные на предупреждение преступлений в студенческой среде.

Преподавательским составом учебных учреждений изучается обстановка в студенческих коллективах, проводится необходимая работа со службами безопасности, пресекаются попытки создания различных объединений, движений и отрядов экстремистской направленности, религиозных сект и реакционных течений, проводится разъяснительная работа к отказу от участия в групповых и насильственных акциях, формированию толерантности к представителям других национальностей и иностранным студентам, обеспечивается контроль за издательской деятельностью, пресекаются попытки распространения среди студентов литературы и агитационных материалов экстремистского содержания, в том числе доставляемых извне. Не допускаются случаи сдачи в аренду в студенческих городках помещений непрофильным организациям, размещения в общежитиях трудовых мигрантов.

В результате проведенных мероприятий установлено, что неформальные молодежные организации на общественную жизнь в студенческой среде высших учебных заведений республики влияния не оказывают.

В каждом высшем учебном заведении республики на проректоров возложены обязанности по взаимодействию с МВД. Ежемесячно проводятся рабочие встречи руководства ВУЗов и МВД.

В образовательных учреждениях республики инспекторами ОДН ОВД постоянно проводятся беседы с учащимися и лекции с родителями о недопустимости участия несовершеннолетних в несанкционированных митингах, акциях, шествиях, других противоправных экстремистских акциях. Для формирования негативного отношения к экстремистским молодежным объединениям в учебных учреждениях республики с несовершеннолетними учащимися, в том числе и с состоящими на учете в милиции проводятся лекции и бесед по военно-патриотическому воспитанию с разъяснением норм уголовного и административного законодательства. Также проводится разъяснительная работа с педагогическими коллективами учебных учреждений республики по выявлению несовершеннолетних, относящихся к различным неформальным группировкам, а также по усилению профилактики экстремизма в проведении работы с подростками, состоящими на профилактических учетах.

С целью выявления неформальных молодежных объединений экстремистского толка, установления новых участников молодежных группировок и постановки их на профилактический учет инспекторами ОДН УВД, ГО-РОВД по УР совместно со службами уголовного розыска и участковыми уполномоченными милиции на плановой основе проводятся рейды по местам концентрации молодежи.

Удмуртская Республика относится к числу политически активных регионов России, на ее территории действуют 17 региональных отделений политических партий. Не все партии, действующие в Удмуртии, одинаково значимы по политическому весу и по уровню своей политической активности. Традиционно наибольшее влияние в республике имеют политические партии: «Единая Россия», «КПРФ», «ЛДПР».

В течение 2009-2010 годов общественно - политическая ситуация в Удмуртской Республике в целом оставалась стабильной. Основное количество прошедших массовых акций носили праздничный, культурный и спортивный характер.

В тоже время, в указанный период времени состоялся ряд протестных акций, связанных с ростом тарифов и цен на услуги жилищно-коммунального комплекса, продукты питания и энергоносители.

Из анализа ситуации, связанной с протестными движениями в Удмуртии следует, что данные движения в регионе ориентировочно начались в январе 2005года, после вступления в силу закона № 122-ФЗ «О монетизации льгот» от 22.08.2004года. Данный закон вызвал негативную реакцию в стране в целом, в том числе и Удмуртии, что послужило созданию Координационного совета протестного движения в республике, который возглавил руководитель регионального отделения КПРФ Фефилов В.Н.

К данному движению примкнул К., который в 2005 году возглавил так называемый Координационный совет Гражданских Действий[1]. После возглавления господином К. КСГД протестные акции (пикетирования, митинги, шествия) в Удмуртской Республике стали проводиться регулярно с использованием в среднем около 300-т человек.

При проведении протестных акций К. выражается недовольство в отношении руководства республики. С целью освещения своей деятельности активно используется собственное информагенство.

В целом, оперативная обстановка по линии противодействия проявлениям экстремистской направленности на территории Удмуртской Республики сохраняет стабильность. Комплекс мероприятий осуществляется во взаимодействии с представителями УФСБ, УФСИН, УФМС России по УР и направлен на удержание ситуации под контролем.

Демократизация всех сторон жизни российского общества, предпринятая в короткие сроки и в больших масштабах, объективно не могла не вызвать, наряду с позитивными результатами, и негативных последствий.

[1] Далее - КСГД

Распространение радикальных и экстремистских идей – это своего рода «рента», которую наше общество платит за быструю либерализацию и деидеологизацию общественной жизни. Сейчас настало время прилагать усилия к консолидации здоровых сил общества с тем, чтобы плодами демократии не воспользовались ее противники.

Международный опыт показывает, что только запретительными мерами разрешить проблему экстремизма невозможно. Для преодоления этого негативного явления необходимо консолидировать общество принять меры, направленные на оздоровление социально-политической и экономической обстановки в стране. Расширение слоя социально благополучной части населения будет способствовать сокращению числа потенциальных участников экстремистских движений.

Тем не менее, правоохранительные органы и, в первую очередь, органы внутренних дел, как наиболее многочисленное и максимально приближенное к населению звено правоохранительной системы должны в полной мере использовать все возможности, которые им предоставляет законодательство в деле предупреждения распространения идей экстремизма, пресечения экстремистских проявлений.

Литература

1. Конституция (Основной закон) Российской Федерации. - М.: Юридическая литература, 2008.

2. Федеральный закон "О противодействии экстремистской деятельности" от 25 июля 2002 г. № 144-ФЗ.

3. Уголовный кодекс Российской Федерации. - М.: Норма, 2008.

4. Послание Президента Российской Федерации от 12.11.2009г. – М: Российская газета № 52, 2009г.

5. Борисов А.Ф. Противодействие политическому и религиозному экстремизму в органах внутренних дел: Методические рекомендации. – СПб., 1999.

6. Михайлов В. Правовое обеспечение противодействия экстремизму//Российская юстиция. – 2002. - № 7. – С. 9 – 11.

7. Петрова Т. А., Попченко А. Р. Предупреждение правонарушений со стороны молодежных неформальных объединений экстремистской направленности. Всероссийский научно-исследовательский институт. Методическое пособие. – М., 2006.

ОСНОВНЫЕ НАПРАВЛЕНИЯ ПРЕДУПРЕЖДЕНИЯ ЭКСТРЕМИЗМА И ТЕРРОРИЗМА В СЕВЕРО-КАВКАЗСКОМ РЕГИОНЕ

А.М. Абдулатипов (Центр профессиональной подготовки МВД по Республике Дагестан).

Сохраняющаяся угроза диверсионно-террористических актов, масштабная распространённость ячеек террористической сети, «необъявленная война» в отношении сотрудников правоохранительных органов и военнослужащих, самовоспроизводящий потенциал экстремистского подполья в Северо – Кавказском регионе определяет противодействие экстремизму и терроризму приоритетным направлением деятельности органов государственной власти и местного самоуправления, общественности, духовенства. Об этом, в первую очередь, свидетельствует до предела повышенная степень общественной опасности террористического подполья (убийство Министра внутренних дел по Республике Дагестан и заместителя Муфтия Духовного управления мусульман Дагестана, посягательство на Президента Республики Ингушетии и др.). Только по Республике Дагестан в 2008 г. зарегистрировано по статье 205 УК РФ – 4 (за 2007 г. -1) преступления, 208 УК РФ – 46 (26), 317 УК РФ – 100 (90). А в 2009 году ситуация ещё более усугубилась. Всего с начала года зарегистрировано 38 преступлений террористической направленности: по статье 205 УК РФ – 6, организаций и участий в незаконных вооружённых формированиях - 32. Кроме того совершено 154 посягательств на сотрудников правоохранительных органов и военнослужащих, что на 86 случаев больше чем за 2008 год в целом.

Как указывает Уолтер Лакюэр, главный миф о террористах заключается в том, что они бедны, голодны и лишены человеческих желаний. Без финансовой поддержки – да, но современный терроризм, как правило, - большой бизнес. Доходы, к примеру, Организации освобождения Палестины составляют 150-200млн. долларов США в год. Официальные лица организации получают 5000 тысяч долларов в месяц и более, имеют шале и счета в Швейцарии.[1]

В этой связи главная задача в борьбе с терроризмом состоит не в выявлении и пресечении отдельных террористических преступлений, а несколько шире – пресечении террористической деятельности как таковой, важную роль, в существовании которой играет ее финансовая основа, дающая возможность терроризму, его людским и материальным ресурсам воспроизводиться.

Отслеживание финансовых потоков представляется весьма трудной задачей, поскольку действующие методики финансового контроля рассчитаны на технику отмывания денег, полученных преступным путем, связанную с «подозрительными операциями». Вместе с тем определенные шаги в рамках деятельности международных организаций уже сделаны. Международное сообщество признало угрозу со стороны финансирования терроризма. В частности это выразилось в том, что европейский союз спонсировал конференцию по этой теме в Люксембурге (1997 год) и семинар в Вене (1998 год). В 1999 году ОАГ провела в

1 Laquer Walter. Terrorism – A Balans Sheet // The Terrorism Reader: A Historical Anthologi. Edited by Walter Laquer. Philadelpfia, 1978. P. 251-267.

Аргентине Вторую Международную конференцию по терроризму, где среди выработанных предложений по противодействию терроризму содержались и рекомендации государствам ОАГ, направленные на сдерживание финансирования терроризма. Венцом поиска эффективных путей противодействия финансирования терроризма стали рекомендации, выработанные в октябре 2001 года в Вашингтоне на состоявшемся внеочередном пленарном заседании ФАТФ (Международная комиссия по борьбе с отмыванием денег), среди которых мы отмечаем следующие:

- принятие немедленных мер по ратификации и имплементации соответствующих документов ООН;
- криминализация финансирования терроризма, террористических актов и террористических организаций;
- замораживание и конфискация террористических активов;
- предоставление возможно более широкого круга помощи правоохранительным органам и контрольным учреждениям в вопросах расследования финансирования терроризма;
- ужесточение мер по идентификации владельца как в отношении международных, так и внутренних переводов.

Таким образом, говоря о международном сотрудничестве, мы считаем, что такое сотрудничество должно проходить не только на уровне правоохранительных ведомств, занимающихся борьбой с терроризмом, но и на уровне финансовых министерств, а также с представителями компетентных правительственных структур и бизнеса.

Определенную перспективу международного сотрудничества мы видим и в информационном сотрудничестве. Важнейший шаг в этом направлении сделан правоохранительными органами Республики Дагестан и Азербайджана, состоящий в налаживании обмена информацией в рамках соглашений о взаимодействии в сфере противодействия террористическим и экстремистским проявлениям на приграничных территориях и обмену информацией о лицах, представляющих оперативный интерес, а также оказании взаимной помощи в розыске опасных преступников.

Среди важнейших сфер сотрудничества в плане противодействия терроризму некоторые практики указывают на необходимость налаживания взаимодействия в пограничном контроле ввоза/вывоза валют, координации финансово- разведывательной деятельности, оптимизации внутригосударственной системы контроля за лицензированием сферы финансовых услуг и внешних и внутренних контрольных механизмов при осуществлении финансовых операций.[1]

Наконец, следует особо сказать о необходимости сотрудничества с мусульманскими странами, имеющими большой опыт борьбы с терроризмом и, в частности, Турцией. Как представляется, разница юрисдикций, социально-экономической и политической ситуаций в наших странах не должна заслонять главного – общих проблем и обязанностей по борьбе с преступностью, особенно с ее наиболее опасными организованными и транснациональными формами.

Направления сотрудничества могут быть самыми различными:

- фактическая реализация всех договоренностей, достигнутых на встречах глав государств по проблемам борьбы с транснациональной преступностью;
- обмен представляющей взаимный интерес оперативно-розыскной, справочной, криминалистической и иной информации;
- проведение по запросам заинтересованных сторон оперативно-розыскных мероприятий и отдельных процессуальных действий по делам такой категории;
- обмен опытом работы, в том числе путем проведения аналогичных встреч, конференций и семинаров;
- планирование и осуществление скоординированных мероприятий, включая в необходимых случаях и проведение «контролируемых поставок» оружия, наркотиков и т.п.;
- издание совместного бюллетеня по текущим вопросам борьбы с терроризмом, а также о положительном опыте пресечения, раскрытия и расследования террористических актов;
- обмен законодательными актами, методическими рекомендациями, а также содействие в приобретении учебной и научной литературы по этим вопросам;
- содействие в подготовке и повышении квалификации кадров, в том числе путем организации стажировок в специализированных подразделениях по борьбе с терроризмом;
- проведение совместных научных исследований, представляющих взаимный интерес;
- оказание правовой помощи путем обеспечения участия официальных представителей заинтересованной стороны в производстве расследования конкретного дела;
- оказание помощи в розыске за рубежом денежных средств и имущества, нажитого преступным путем.

Особая статья сотрудничества должна состоять в обмене опытом. Представляется, что в деле борьбы с терроризмом США пошли значительно дальше. Заслуживает внимания, к примеру, американский опыт действия Программы защиты свидетелей, а также инструкция Генерального атторнея США, регламентирующая тайную операцию, которая допускает «приглашение к совершению противозаконных действий и создание возможностей для противозаконных действий», то такого рода мероприятия прямо запрещены российским

[1] См.: Устинов В. Конвенция о борьбе с финансированием терроризма // Рос. юстиция. – 2002. - №3. – 8-11.

законом об оперативно-розыскной деятельности. Вместе с тем, думается, что без подобных оговорок в российском законодательстве, такие эффективные специальные мероприятия как оперативное внедрение, контролируемая поставка, создание и использование легендируемых предприятий становится невозможным.

Важным направлением предупреждения терроризма является профилактическая деятельность правоохранительных органов, которые до сих пор борются с террористической преступностью, что называется, «по факту». В этой связи считаем правильным борьбу этих органов направить на более ранние стадии террористической преступной деятельности и, в частности, на разрушение связей между ячейками преступных группировок и с лидерами так называемого «Кавказского Амирата» под руководством Доку Умарова. В результате целенаправленной профилактической и оперативно-розыскной работы правоохранительных органов и помощи от населения в текущем году в Дагестане предотвращено 10 терактов.

Назрела также проблема повышения профилактического потенциала контртеррористических операций, которые проводятся под руководством региональных оперативных штабов Национального Антитеррористического Комитета (НАК) РФ с привлечением сил и средств группы оперативного управления (ГРОУ), в состав которого входят подразделения различных правоохранительных и силовых ведомств, представители органов государственной власти и местного самоуправления. Анализ результатов деятельности оперативных штабов показывает, что главные недостатки обусловлены, в основном, слабостью оперативно-розыскной составляющей, отсутствием упреждающей информации о готовящихся преступлениях террористической и экстремистской направленности, посягательствах на сотрудников правоохранительных органов и военнослужащих. В связи с этим основное внимание необходимо уделить вопросам совершенствования разведывательной деятельности соответствующих служб.

Важным решением в повышении эффективности деятельности правоохранительных органов в противодействии экстремизму и терроризму могло бы стать организация полноценного банка данных по всем вопросам, касающимся деятельности террористических и экстремистских группировок, а также:

- принятие действенных мер к улучшению деятельности оперативных подразделений и спецслужб МВД и ФСБ по установлению лиц, совершивших преступления, и розыску преступников;
- дальнейшее совершенствование и усиление координации правоохранительных органов, т.к. раскрытие преступлений данной категории предполагает активное взаимодействие всех правоохранительных органов;
- возможность применения контролируемых активных (в определенной мере противоправных) действий в отношении лидеров и членов террористических группировок, в частности некоторое санкционированное ограничение процессуальных прав подозреваемых и обвиняемых в совершении террористических актов;
- Активизировать работу структурных подразделений Национального Антитеррористического Комитета и постоянно действующих межведомственных следственно-оперативных групп по борьбе с терроризмом;
- продолжение активных действий по окончательному разгрому на территории Северокавказского региона ячеек террористической сети и непримиримых сепаратистов, как социальной, идеологической и материальной базы поддержки и распространения религиозного и политического экстремизма на Северном Кавказе, а также как опорной базы международного терроризма;
- выявление и пресечение деятельности внешних деструктивных и подрывных сил, действующих под прикрытием различных международных благотворительных фондов, общественных и религиозных организаций (в прошлом году судами удовлетворены три заявления прокурора РД о признании недействительными регистрации трех представительств международных благотворительных организаций).

Как отметил Министр внутренних дел России Р. Г. Нургалиев, системное применение инновационных методов, наукоёмких, технических, информационно - аналитических, телекоммуникационных систем умножает возможности сокращения преступности, в том числе террористической направленности. В последние годы серьёзное внимание уделяется оборудованию патрульных автомобилей средствами связи и специальной техникой на основе современных информационных и телекоммуникационных технологий, спутниковыми навигационно-мониторинговыми системами "ГЛОНАСС", оборудованию диспетчерских пунктов при дежурных частях ОВД системами видеонаблюдения и установлению системы мониторинга мобильных экипажей милиции. Создается система управления мобильными нарядами для устойчивой регулярной связи "человек - милиция". Развивается единая информационно-телекоммуникационная система, которая обеспечивает доступ к специализированным базам данных федерального и регионального уровней и позволяет мгновенно реагировать на происшествия. Внедряются центры управления нарядами для оперативного руководства и координации действий нарядов различных подразделений милиции. Всё это способствует повышению оперативности получения, обработки и анализа информации о состоянии криминогенной обстановки.

Борьба с терроризмом – это не монополия специальных служб и правоохранительных органов. Она должна стать предметом заботы всех органов государственной власти и управления, всего гражданского общества.

Важнейшим направлением нормализации криминогенной обстановки, предупреждения разрастания террористической угрозы в стране, особенно в условиях Северного Кавказа, является принятие и реализация

материально и финансово обеспеченной комплексной программы, включающей меры политического, экономического, социального, идеологического и правового характера. Именно с такого рода решениями мы связываем осуществление задач ранней профилактики терроризма, которая состоит в самопроизвольном разрешении большинства сложившихся в обществе конфликтов интересов.

Анализ имеющегося законодательства, направленного на борьбу с терроризмом в регионе, позволяет думать, что основной отдачи здесь следует ждать не столько от совершенствования законодательства, сколько от повышения эффективности правоприменительной деятельности. Именно несоответствие правоприменительной практики уровню задач, стоящих в данной области государственной политики, является главным фактором, препятствующим эффективной борьбе с нарушениями соответствующего законодательства и успешной профилактики правонарушений. В подтверждение данного обстоятельства можно привести тот факт, что в порядке надзора по делам в отношении задержанных в ходе антитеррористической операции в кадарском аклаве, губденской зоне, рассмотренным городскими и районными судами, принесено 59 протестов на отмену приговоров в виду мягкости назначенного наказания и необоснованной квалификации содеянного. Все протесты удовлетворены Президиумом Верховного суда республики. Однако в последующем Судебной коллегией по уголовным делам Верховного суда России по жалобам адвокатов осужденных постановления Президиума Верховного суда РД изменены или отменены по 18 делам.

Другой факт посредственности правоприменительной практики в части применения ст. 5 Закона Республики Дагестан «О запрете ваххабитской и иной экстремистской деятельности на территории Республики Дагестан» (по имеющимся в органах прокуратуры данным), которая полностью отсутствует. Должностными лицами администраций различных уровней протоколы о таких административных правонарушениях не составляются. На наш взгляд, бездействие Республиканского Закона обусловлено решительным противодействием (после августовских - сентябрьских событий) самого населения республики сторонникам «ваххабизма» и активными действиями органов внутренних дел по пресечению малейших антиконституционных проявлений и задержанию виновных в порядке, предусмотренном уголовно-процессуальным законом.

Возвращаясь к теме формирования законодательной базы, следует указать на то, что законодатель с учетом щепетильности данного вопроса должен особенно продуманно делать отдельные шаги по искоренению обстоятельств, способствующих терроризму, ибо меры противодействия известному феномену могут породить в свою очередь иные социальные конфликты. Так ст. 2 Закона Республики Дагестан «О запрете ваххабитской и иной экстремистской деятельности на территории Республики Дагестан» указывает на то, что «обучение граждан Республики Дагестан в религиозных учебных заведениях за пределами Республики Дагестан и Российской Федерации допускается только по направлению органа управления республиканской организации, согласованному с государственным органом по делам религии Республик Дагестан». Данная норма ущемляет конституционное право на свободу совести и свободу вероисповедания и противоречит ст. 5 Федерального закона «О свободе совести и религиозных объединениях», согласно которой «каждый имеет право на получение религиозного образования по своему выбору индивидуального или совместно с другими». На наш взгляд, такая правовая некорректность является весьма опасной не только потому, что она ущемляет права и свободы граждан, но и потому, что в сложившихся условиях она может стать лишним аргументом для тех, кто заинтересован в эскалации религиозного экстремизма.

Наконец, считаем назревшим дальнейшую разработку закона «О защите личной и общественной нравственности в Республике Дагестан», «О чрезвычайном положении», разработку Федерального закона «О борьбе с политическим экстремизмом». В части применения уголовного закона считаем назревшими руководящие разъяснения Пленума Верховного суда РФ по делам о терроризме, так как существует проблема неадекватной оценки фактически совершаемых деяний террористической направленности. К примеру, преступления, которые совершаются в рамках систематического, организованного нападения на гражданские населения, государственные институты власти (организация незаконного вооруженного формирования или участия в нем, вооруженный мятеж, насильственный захват власти или насильственное удержание власти) чаще всего имеют своей целью свержение существующей законной власти, предполагают непосредственное вооруженное сопротивление представителям власти, выполнение боевых заданий командования незаконного вооруженного формирования по разведке, диверсиям, террористическим актам. Вместе с тем, как правило, в рамках таких деяний доказанными остаются преимущественно преступления против общественной безопасности и общественного порядка (Для примера: В своих выступлениях лидер террористической сети на Северном Кавказе Доку Умаров ставит своей целью отторжение Кавказа от России и создание Кавказского Амирата как шариатского независимого государства).

В деле формирования правовых мер борьбы с терроризмом большое значение имеет правильная расстановка акцентов. Современная практика борьбы с терроризмом ведущих стран мира, имеющих многолетний опыт борьбы противодействия терроризму как внутри своей страны, так и за ее пределами, свидетельствует о новом направлении в уголовной политике, центр тяжести которой все чаще переносится в сферу уголовного судопроизводства. Действительно, как показала практика, ресурсы уголовного права в борьбе с терроризмом весьма ограничены: остановить развитие террористической деятельности не может ни угроза смертной казни, ни длительные сроки лишения свободы. Вместе с тем, опыт модернизации уголовного судопроизводства Великобритании и США свидетельствует о перспективности данного направления предупредительной деятельности, остовом которой является постоянная работа по расширению понимания

терроризма как социально-негативного феномена, увеличения списка запрещенных организаций, ограничение прав отдельных граждан и организаций, подозреваемых в причастности к терроризму, регулирования правового режима чрезвычайного положения[1]. В Великобритании в Законе «О терроризме» 2000 года дошло до того, что была отменена презумпции невиновности в отношении лиц, подозреваемых в терроризме и переносе, таким образом, бремени доказывания невиновности на самих подозреваемых. Больше того, в упомянутом законе установлена ответственность за: 1)ношение одежды с символами запрещенных организаций (ИРА и др.); 2) сбор информации, которая может быть использована для совершения актов терроризма; 3) сокрытие любой информации, которая может способствовать раскрытию преступлений, связанных с совершением террористических актов. Заслуживает внимания также положения данного закона, согласно которому в Северной Ирландии практически отменено действие суда присяжных заседателей. Представляется, что актуальна и своевременна инициатива Президента РФ Д. А. Медведева по отмене действия уголовного судопроизводства с участием присяжных заседателей по делам о преступлениях террористической направленности, особенно для республик Северокавказского региона, а также возможность рассмотрения таких дел в других регионах. (В качестве отрицательного примера можно привести признание судом присяжных невиновным гражданина О., который обоснованно обвинялся в посягательстве на Министра внутренних дел РД Магомедтагирова А. М.)

Серьезная нравственная ответственность за разрастание насилия в стране лежит и на отечественных средствах массовой информации, формирующих мировоззрение миллионов граждан. К сожалению, здесь в условиях всеобъемлющей коммерциализации весьма часто верх берет не гражданская позиция и высокий профессионализм, а стремление любым путем повысить тираж печатного издания или расширить аудиторию телезрителей. Это вполне вписывается в расчеты террористов, поскольку отличительной чертой терроризма является публичность. Действительно поскольку терроризм рассчитан на массовое восприятие, постольку позитивный вклад средств массовой информации в борьбу с терроризмом может быть значительным, как впрочем, и вклад негативный. Представляется опасным делание из террористов жертв сложных жизненных обстоятельств, а их действия законным результатом непростого существования. Больше того, огромный негатив мы связываем с формированием некоторыми журналистами из террористов образа «народного героя». Так, например, отдельные журналисты, подчеркивая свое стремление «объективно» разобраться в происходящем в республике, по существу, оправдывали террористов. Как не вспомнить, что некоторые представители средств массовой коммуникации (особенно в газете «Черновик») до сих пор любят восхвалять лидеров террористической сети, показывают их как благородных борцов за свободу народа и последователей «чистой» религии. Одновременно на единичных примерах сотрудников правоохранительных органов представляют как профессионально неподготовленных, массово коррумпированных, безответственных, нравственно нечистоплотных.

При этом следует отметить, что в цивилизованном обществе террористы могут только мечтать о возможности получить доступ к средствам массовой информации, ибо на это, как правило, террористы рассчитывают. СМИ выступает как бы специальным передаточным механизмом («ретранслятором») между террористами и адресатами террора.

В этой связи нам представляется, что средства массовой информации Северного Кавказа должны вести планомерную работу по разъяснению сущности и опасности проявлений религиозного, политического, национального и т.п. экстремизма. Тема обеспечения безопасности региона, противодействия экстремизму должна стать главной темой в программах местного телевидения с участием интеллигенции, представителей духовного управления мусульман республики, которые должны осуществлять контрпропаганду идеям экстремизма, особенно среди молодежи. Определенный положительный эффект мы связываем с выступлениями работников правоохранительных органов о проводимой работе по противодействию террористической деятельностью. В целом работа в известном направлении в информационной и пропагандистской сфере требует существенной активизации, избирательности, наполнения конкретным содержанием.

Наконец, следует отметить, что государство в борьбе с терроризмом должно реально оценивать террористические угрозы и принимать адекватные меры по их устранению или смягчению. Так, противодействие конкретным актам терроризма должно сообразовываться с масштабами средовой поддержки. Если такая поддержка не носит широкий характер, то репрессивные меры вполне оправданы. Если же такая поддержка есть, жесткие санкции, в частности наказание преступников смертной казнью, войсковые операции и т.п. крайние меры вызовут еще большее противодействие, организацию новых экстремистских групп и пополнение уже имеющихся. В этой связи мы считаем глубоко продуманными действия государства по продолжению специальной комплексной профилактической операции с привлечением дополнительных сил и средств из других регионов в Дагестане и, в частности, в Губденской зоне и Унцукульском районе, где была правильно оценена обстановка, население республики было психологически подготовлено к соответствующим мерам в отношении так называемых адептов «чистого ислама», которые фактически являются бандитами и рэкетирами.

[1] См. подр.: Ведерникова О.Н. Отказ от традиционных принципов уголовного судопроизводства как форма реагирования на угрозу терроризма / Реагирование на преступность: концепции, закон, практика. Сб. науч. трудов. – М. – 2002. – С. 60-63.

Вместе с тем, считаем, что осуществление политики в отношении Северного Кавказа, в целом, не достаточно продуманной. Представляется, что такая политика должна учитывать менталитет горцев, с тем, чтобы избежать судьбы Чечни, войну в которой называют войной цивилизаций. В этой связи, считаем, что эффективное предупреждение религиозного экстремизма в республиках Северного Кавказа во многом зависит от степени осознания многоконфессионального характера России, способности объединения всех конфессий во имя достижения единой цели – формирование истинного правового государства. Но эту роль государство может выполнить только с четко продуманной программой. По мнению Боронбекова С., государство не может стоять в стороне от формирования подлинного религиозного сознания личности. Речь не о прямом вмешательстве, а о содействии обществу, личности в получении достоверного, истинного религиозного образования, доступной правды о религии. В противном случае общество будет наводнено такими лжерелигиозными организациями и сектами, которые могут причинить огромный ущерб государству в целом. Следует остеречься в то же время от иной крайности, тенденции которой обнаруживаются сегодня, когда духовенство, под предлогом противодействия ваххабизму, пытается взять под контроль всю систему образования, воспитания, культуры, СМИ и даже кое-где почти полностью заменить светские органы власти на местах представляет серьезную опасность для цивилизованного светского будущего республики в составе Федерации.

Главенство светских федеральных законов и традиций, праздников, ритуалов государственного и республиканского уровня является гарантом безопасности и стабильности в обществе. Учитывая все это, а также опыт республики в опережающей разработке законов, впоследствии востребованных на федеральном уровне, возможно, было бы целесообразно при подготовке законов учитывать то, что Северный Кавказ, Дагестан - это Россия в миниатюре, только с гипертрофированной экстремистской угрозой.

Практика доказывает необходимость реформирования и структурного переоформления всей мусульманской иерархической пирамиды с учетом обозначившихся естественных процессов.

Духовное управление мусульман Дагестана, считающееся официально главным органом духовной власти, только в последние годы сумела взять под контроль всех процессов в дагестанском мусульманском сообществе. Вместе с тем не в полной мере удалось преодолеть национальной разобщенности. В горных районах стихийно возникла новая форма духовного управления – имаматы, которая в некоторых районах прижилась и остается доминирующей. Возможно, реформировать всю структуру следует, исходя именно из этих уже народившихся реалий. В этом случае необходимо достаточно жестко и четко по всему спектру общественной жизни разграничить компетенцию духовенства и светской власти. Причем, естественно, имамы должны быть подконтрольны и Конституции и законам. Более того, они должны осознавать, что их безопасность и благополучие напрямую связаны с лояльностью власти. Без восстановления этой базовой вертикали не может быть гарантирована безопасность светского государства. Важно, что на этом пути мы не являемся первопроходцами. Турция давно разработала законодательную базу разделения сфер компетенции исламского духовенства и светской власти. Система эта уже апробирована и успешно действует, позволяя Турции, при сохранении основных исламских ценностей, динамично интегрироваться в современное мировое сообщество. Подобную вертикаль в последние годы активно пытаются установить и власти Азербайджана.

В этой связи вполне обоснованной считаем встречу Президента Российской Федерации Д. А. Медведева с государственными руководителями и муфтиями духовных управлений мусульман Дагестана, где акцент был сделан на разъяснение истинной природы терроризма на Кавказе. Президент России справедливо отметил, что нет так называемого «исламского терроризма», что преступников необходимо называть бандитами и террористами, а не «исламистами». Впервые на столь высоком официальном уровне признано, что религия используется членами бандподполья как ширма, что ни ислам, ни другая мировая религия не имеет отношения к терроризму.

Не меньшую угрозу представляют и те, кто лоббирует интересы бандподполья, занимая должности в органах государственной власти и муниципалитете, по сути являясь мафиозными структурами, которые также прикрываются религиозной оболочкой. В связи с этим заявление Президента России в Сочи о необходимости полного уничтожения бандитов и его призыв к отказу идентифицировать или называть их как «исламских террористов» является своевременным и актуальным в сфере идеологического противодействия мафиозным кланам.

Использование богатого отечественного опыта работы с мусульманским духовенством и творческое освоение опыта мусульманских республик СНГ и стран дальнего зарубежья, особенно в области законодательной системы позволят выстроить заново всю систему отношений многоконфессионального и полиэтничного государства и религии и тем самым устранить базу для терроризма.

КИБЕРТЕРРОРИЗМ: НАПРАВЛЕНИЯ ПРОТИВОДЕЙСТВИЯ

З.О. Гецелев (Академия управления МВД России)

Современные международные конфликты приобретают новые формы, опираются на технические средства, но формально они не являются оружием. Это могут быть войны без применения вооружений и военной техники и без осуществления силового воздействия, полностью основывающиеся на применении информационных и сетевых технологий. Такие формы противостояния могут быть не менее разрушительными,

чем традиционные вооруженные конфликты[1].

Одной из главных угроз международной безопасности стал терроризм, который поставил перед многими странами задачу организации адекватного противодействия. На международном уровне терроризм давно проявил себя как феномен всемирного характера, не признающего границ. Особенно это характерно для его новых технологических или высокотехнологических форм. В полной мере это распространяется и на новые формы его проявления – кибертерроризм или, как его часто еще называют, электронный терроризм. По существу, эта новая форма терроризма представляет собой разновидность использования высоких технологий в преступных целях. Анализ мировых тенденций развития кибертерроризма с большой долей вероятности позволяет прогнозировать, что его угроза с каждым годом будет возрастать.

Термин «кибертерроризм» ввел в середине 1980-х гг. старший научный сотрудник американского Института безопасности и Разведки (Institute for Security and Intelligence) Бэрри Коллин (Barry Collin), и обозначал он террористические действия в виртуальном пространстве. Тогда этот термин использовался лишь для прогнозов на будущее. Сам автор термина предполагал, что о реальном кибертерроризме можно будет говорить не раньше, чем в первые десятилетия XXI века.

Однако первые кибератаки были зафиксированы уже в начале 1990-х гг. В 1996 г. специальный агент Федерального Бюро Расследований (ФБР) Марк Поллит (Mark Pollitt) предложил определять кибертерроризм как «преднамеренные, политически мотивированные атаки на информационные, компьютерные системы, компьютерные программы и данные, выраженные в применении насилия по отношению к гражданским целям со стороны субнациональных групп или тайных агентов»[2]. В настоящее время Центр защиты национальной инфраструктуры (National Infrastructure Protection Center), находящийся под управлением DHS, определяет кибертерроризм как «уголовный акт, совершенный при помощи компьютеров, направленный на насилие, смерть и/или разрушение, ради политических целей».

Некоторые эксперты в области безопасности считают, что компьютерная атака может быть определена как кибертерроризм только в том случае, если последствия такой атаки достаточно разрушительны и могут быть приравнены к последствиям от традиционных террористических актов (человеческим жертвам, увечьям, сбоям в работе энергоснабжения, крушениям самолетов или потере доверия к финансово-кредитной системе страны)[3].

В отличие от традиционного, этот вид терроризма использует в террористических акциях новейшие достижения науки и техники в области компьютерных и информационных технологий, радиоэлектроники. Более того, можно утверждать, что компьютерный терроризм уже стал опасным проявлением высокотехнологического терроризма, а информационные технологии стали его новой технологической базой.

Исследователи М.Дж. Девост, Б.Х. Хьютон, Н.А. Поллард определяют информационный терроризм как сознательное злоупотребление цифровыми информационными системами, сетями или компонентами этих систем или сетей в целях, которые способствуют осуществлению террористических операций или актов[4]. По нашему мнению, следуя этому определению, можно выделить два вида кибертерроризма:

1) непосредственное совершение террористических действий с помощью компьютеров и компьютерных сетей;

2) использование киберпространства террористическими группами в организационно-коммуникационных целях и с целью шантажа, но не для непосредственного совершения терактов.

Первый вид соответствует объединению понятий «киберпространство» и «терроризм» и представляет собой умышленную атаку на компьютеры, компьютерные программы, компьютерные сети или обрабатываемую ими информацию, создающую опасность гибели людей, причинения значительного имущественного ущерба либо наступления иных общественно опасных последствий. Например, перехват управления военным или инфраструктурным объектом в целях нарушения общественной безопасности, устрашения населения либо оказания воздействия на принятие решений органами власти путем угрозы осуществления аварии (катастрофы)[5].

С точки зрения рассматриваемой в данной работе проблемы – борьбы с международным терроризмом – в определении кибертерроризма нас интересует прежде всего его политическая мотивированность (а не хулиганство, воровство или мошенничество). Поэтому мы не распространяем понятие «кибертерроризма» на преднамеренные, но политически немотивированные преступления хакеров, имеющие целью нанесение материального ущерба, саботаж информационных систем, мошенничество или злоупотребление полученной информацией.

Дороти Деннинг (Dorothy Denning), профессор компьютерных наук Джорджтаунского университета и

---

[1] Приветствие Министра иностранных дел России С.В.Лаврова участникам научно-практической конференции «Наука, технологии и международные отношения в эпоху глобализации: роль образования и инноваций», Москва, МГИМО, 24 апреля 2006 года

[2] *Красавин С.* «Что такое кибертерроризм?» // http://rr.sans.org/infowar

[3] CRS report 32114. Computer attack and Cyber Terrorism: Vulnerabilities and Policy Issues for Congress. October 17 2003

[4] *Томас Т.Л.* Сдерживание асимметричных террористических угроз, стоящих перед обществом в информационную эпоху// Мировое сообщество против глобализации преступности и терроризма. Материалы международной конференции. М., 2002.

[5] *Татьяна Тропина* «Киберпреступность и кибертерроризм» http://www Crime.vl.ru; Голубев В.А. «Кибертерроризм» — миф или реальность? Голубев В.А. Кибертерроризм как новая форма терроризма? http://www.crime-research.org

один из самых авторитетных экспертов в области компьютерной преступности и кибербезопасности, в своей книге «Активность, хактивизм и кибертерроризм: Интернет как средство воздействия на внешнюю политику» говорит о кибертерроризме как о «противоправной атаке или угрозе атаки на компьютеры, сети или информацию, находящуюся в них, совершенной с целью принудить органы власти к содействию в достижении политических или социальных целей»[1]. Она полагает, что для международных террористов информационные средства нападения по сравнению с «физическими» представляют некоторое преимущество. С их помощью можно действовать отдаленно и анонимно, они дешевы, не требуют опасных в транспортировке взрывчатых веществ. Такие теракты с высокой вероятностью получают широкую огласку в СМИ.

К первому виду кибертерроризма примыкают все осуществляемые с помощью Интернета, так называемые, «информационные» правонарушения против Конституции (антиконституционные призывы, угрозы конституционным правам и свободам человека и гражданина, распространение устрашающих слухов, угрозы информационному обеспечению государственной политики и др.).

Второй вид кибертерроризма – использование информационного пространства террористическими группами в организационно–коммуникационных целях (но не для непосредственного совершения терактов), проведение теоретического, военного, теологического обучения и пропаганды, а также рекрутирование новых членов и обеспечение связи между отдельными ячейками. Существует несколько способов, с помощью которых террористические группы используют интернет в своих целях:

1. Сбор информации, необходимой для планирования терактов.

2. Сбор денег для поддержки террористических движений (в том числе путем вымогательства и шантажа).

3. Распространение агитационно-пропагандистской информации о террористических движениях, их целях и задачах, намеченных действиях, формах протеста, обращение к массовой аудитории с сообщениями о признании своей ответственности за совершенные террористические акты и т.п.

4. Осуществление информационно–психологического воздействия на население с целью шантажа, создания паники, распространения дезинформации и тревожных слухов.

5. Осуществление организационной деятельности, например, размещение в открытом доступе и рассылка открытых и зашифрованных инструкций (информации о взрывчатых веществах и взрывных устройствах, ядах, отравляющих газах, а также инструкций по их самостоятельному изготовлению), сообщений о времени встреч заинтересованных людей и проч.

6. Анонимное привлечение к террористической деятельности соучастников, например, хакеров и представителей бизнеса, оказывающих различные информационные услуги на коммерческой основе и не отдающих себе отчета в том, кто и почему эти услуги оплачивает.

7. Возрастающие технологические возможности применения коммуникационных технологий для планирования и координации своих действий создают основу для перехода к менее четким организационным структурам, расширения потенциала малых террористических групп, намеренных осуществлять свои операции децентрализованно.

Американский исследователь Дэн Вертон (Dan Verton), автор книги «Черный Лед: Незримая Угроза Кибертерроризма» (Black Ice: The Invisible Threat of Cyberterrorism), считает, что многие террористические организации создали в интернете базы разведывательных данных. Известно, например, что японская террористическая группировка «Аум Синрике», которая провела газовую атаку в токийском метро в 1995 г., перед этим создала компьютерную систему, которая была способна перехватывать сообщения полицейских радиостанций и отслеживать маршруты движения полицейских автомобилей.

Чаще всего террористы используют интернет для связи, пропаганды, привлечения сочувствующих и пр. По данным исследования, проведенного институтом United States Institute for Peace (USIP), Всемирная Сеть является идеальной средой для деятельности террористов, поскольку доступ к ней крайне легок, в ней просто обеспечить анонимность пользователей, она никем не управляется и не контролируется, в ней не действуют законы и не существует полиции. Если в 1998 г. примерно половина из 30‑ти организаций, которых США причисляли к террористическим, обладали своими сайтами, то ныне в Сети представлены абсолютно все известные террористические группы, которые публикуют свои материалы, по меньшей мере, на 40 языках.

Наиболее опасным способом использования интернета (кибертерроризм второго типа) является размещение на сайтах руководств по изготовлению бомб, оружия, организации терактов и пр. Пионерами в этом деле были анархисты: они еще в 1950‑е гг. создали подобное пособие «Поваренная Книга Анархиста», которую с конца 1980‑х гг. активно популяризуют в интернете. Владельцы сайтов, которые вывешивают подобные инструкции, обычно избегают наказания, утверждая, что не они являются авторами руководств и не призывают использовать данную информацию на практике. По данным Бюро по контролю за алкоголем, табаком и огнестрельным оружием (Bureau of Alcohol, Tobacco, and Firearms), за период с 1985 по 1996 гг. спецслужбы США расследовали по меньшей мере 30 дел, связанных со взрывами бомб, когда бомбисты получали необходимые знания, изучая информацию, размещенную в Интернете[2].

В начале XXI века на проблемы национальной безопасности администрацию президента Дж.Буша

[1] *Denning D.E.* Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy //http://www.nautilus.org/info-policy/workshop/papers/denning.html.

[2] «Терроризм в Сети» Материал портала agentura.ru

заставили обратить серьёзное внимание террористические акты, произошедшие 11 сентября 2001 г. После них Америка вновь почувствовала себя уязвимой; в США была осознана потребность в повышении уровня национальной безопасности.

Но террористическим нападениям подверглись не только башни Торгового центра в Нью–Йорке, – Соединённые Штаты подверглись также атакам кибертеррористов (в качестве примеров были приведены нацеленные на американские сайты кибератаки вирусов NIMDA и Code Red). IT–преступления стали совершаться чаще, они стали более изощрёнными, причинют больший ущерб. Американскому государству надо было решать задачу обеспечения информационной безопасности страны.

Перед американским государством встала задача обеспечения кибербезопасности страны, то есть обеспечения уверенности в надежной и адекватной работе информационно–коммуникационных компьютерных систем, в том числе: информационной безопасности (information security); обеспечения восстановления нормальной работы системы и информационных ресурсов после возможных аварий, а также после случайных или несанкционированных вторжений.

Через шесть недель после террористических атак на Нью–Йорк и Вашингтон Конгрессом США был принят новый антитеррористический закон США, известный как «Патриотический Акт 2001 года». Этим законом Конгресс ввел новое законодательное понятие «кибертерроризм» и отнес к нему различные квалифицированные формы хакерства и нанесения ущерба защищенным компьютерным сетям граждан, юридических лиц и государственных ведомств, включая ущерб, причиненный компьютерной системе, используемой государственным учреждением при организации национальной обороны или обеспечении национальной безопасности.

Предотвращение компьютерных преступлений было включено в сферу обеспечения национальной безопасности США, а борьба с преступностью в сфере IT технологий стала одним из главных приоритетов политики администрации Дж.Буша. Это потребовало дополнить стратегию национальной безопасности специальным документом – стратегией национальной безопасности США в киберпространстве (принята в феврале 2003 г.). В этом документе официально признается то, о чем раньше говорилось только в кулуарах, в частности, констатируется, что жизнь каждого американца стала слишком сильно зависеть от информационных технологий, от различных составляющих национальной инфраструктуры, которые оказались весьма уязвимыми для кибертеррористов. По мнению федерального правительства США, государство оказалось не готово противостоять подобным угрозам, оно просто не в состоянии обеспечить соответствующими системами компьютерной безопасности все частные банки, энергетические компании, предприятия транспорта и другие компоненты частного сектора. В Стратегии подробно рассматриваются угрозы нанесения возможного ущерба, приводятся рекомендации, как избежать этого ущерба, акцентируется роль государства в противодействии преступлениям, совершаемым с помощью IT–технологий.

Американские специалисты признают, что широкое распространение компьютеров и современных средств связи привело к возрастанию зависимости всех критически важных элементов базисной инфраструктуры экономики страны от нормального функционирования информационных технологий. Поэтому повреждение или разрушение информационных сетей, обеспечивающих нормальную работу транспорта, энергетического хозяйства и прочее, непосредственно воздействует на экономику в целом, которая оказалась «прискорбно незащищенной» и очень уязвимой для террористических атак.

Государство оказалось во многом не готово противостоять террористическим угрозам, оно просто не в состоянии обеспечить соответствующими системами компьютерной безопасности все частные банки, энергетические компании, предприятия транспорта и другие компоненты частного сектора. В правительственных документах отмечается, что в настоящее время с точки зрения безопасности сложились следующие неблагоприятные условия развития информационной инфраструктуры:

-чрезмерная скорость старения технологии;

-безграничность интернета и неадекватность нормативно–правовой базы, регулирующей информационные потоки;

-невозможность идентификации преступника

-ограниченные ресурсы обеспечения кибербезопасности.

В принятом в конце ноября 2002 г. новом Законе об исследованиях в области кибербезопасности (Cybersecurity Research and Education Act of 2002) понятие «кибербезопасности» определяется как научное, техническое, организационное, информационное и иное обеспечение компьютерной и сетевой безопасности, в том числе по следующим направлениям:

– оперативная и административная безопасность систем и сетей;
– инжиниринг систем безопасности;
– системное информационное и программное обеспечение
– криптография;
– оценка угроз и уязвимости компьютеров (сетей), управление рисками;
– безопасность Web–сайта;
– компьютерные действия в случае чрезвычайных ситуаций;
– организация образования и подготовки кадров по кибербезопасности;
– судебные дела, связанные с информацией и компьютерами;
– работа с конфиденциальной информацией.

Суть этого Закона состоит в том, чтобы обеспечить под эгидой Национального научного фонда (National Science Foundation) финансирование и запустить в ВУЗах США реализацию ряда программ, расширяющих подготовку специалистов по кибербезопасности, в частности, программ послевузовской специализации студентов (аспирантуры), а также программ, стимулирующих наиболее продвинутых студентов участвовать в реальных исследованиях и разработках по актуальным вопросам кибербезопасности (так сказать, «на докторском уровне»).

Этим законом NSF уполномочивается финансировать предоставление наиболее продвинутым преподавателям университетов 25 годовых грантов и годичных отпусков для научной работы по тематике кибербезопасности. Имеется в виду проведение такой работы в Агентстве национальной безопасности, Министерстве обороны, Национальном институте стандартов и технологий, исследовательских лабораториях Министерства энергетики и других институтах, работающих по данной тематике. Предполагается предоставление ведущим организациям грантов, имеющих целью ускорение развития инфраструктуры кибербезопасности (при этом организация, которой предоставляется грант, должна выполнить по нему не менее 25% работ). Помимо грантов, на предстоящие четыре года Закон учреждает премии за выдающиеся работы по кибербезопасности, а также повышение качества подготовки кадров по соответствующим специальностям.

В странах Европы идут аналогичные процессы. В разряд приоритетных выдвигается вопрос о правовых и организационных механизмах регулирования использования компьютерных сетей. Первым международным соглашением по юридическим и процедурным аспектам расследования и криминального преследования киберпреступлений стала Конвенция о киберпреступности, принятая Советом Европы 23 ноября 2001г[1]. Конвенцией предусматриваются скоординированные на национальном и межгосударственном уровнях действия, направленные на недопущение несанкционированного вмешательства в работу компьютерных систем.

В России, в качестве базиса для развития международного взаимодействия по парированию угроз информационной безопасности является межправительственное соглашение с республиками Казахстан, Белоруссия и Украина о сотрудничестве в области защиты информации.

Бороться с таким глобальным явлением как кибертерроризм, имеющим отчетливо выраженный трансграничный характер, невозможно без объединения усилий всех заинтересованных государств. И всестороннему развитию международного сотрудничества с зарубежными партнерами придается особое значение. Заместитель генерального прокурора США Джеймс Робинсон в выступлении на международной конференции по компьютерной преступности признал, что правительство не в состоянии справиться с этой угрозой в одиночку[2], а потому в борьбу с компьютерной преступностью, в укрепление национальной информационной безопасности необходимо вовлекать широкие круги бизнеса (то есть пользователей) и содействовать развитию их сотрудничества с государственными структурами.

Со своей стороны министр внутренних дел России генерал армии Рашид Нургалиев, выступая на Международной встрече специалистов-практиков по борьбе с киберпреступностью и кибертерроризмом, которая была организована по инициативе МВД России в рамках председательства РФ в «большой 8», отметил, что задачей этого международного форума является сближение подходов различных государств и выработка совместных практических мер по актуальным вопросам борьбы с киберпреступностью.

Выступление председателя исполкома «Ассоциации документальной электросвязи» Аркадия Кремера «Международное сотрудничество в области информационной безопасности» было посвящено конкретному примеру международного сотрудничества в области обеспечения безопасности инфокоммуникационных сетей и систем – проекту Международного союза электросвязи «Базовые требования информационной безопасности сетевых операторов».

Особое значение для России имеет политическое противодействие использованию информационных технологий в целях, противоречащих уставу ООН. Сегодня очевидно, что в условиях все более взаимосвязанного и взаимозависимого мира только общими усилиями – с участием правительств, институтов гражданского общества, деловых кругов, при важной роли международного научного сообщества – мы сможем противостоять современным угрозам, приобретающим беспрецедентные масштабы, – от глобальных техногенных катастроф и распространения инфекционных заболеваний до угроз международного терроризма и трансграничной преступности[3].

В работах заместителя директора Департамента по вопросам безопасности и разоружения МИД РФ профессора А.В. Крутских говорится о потенциальных возможностях использования информационных технологий в целях, несовместимых с соблюдением принципов отказа от применения силы, невмешательства во внутренние дела государств, уважения прав и свобод человека; а также о том, что «милитаризация информационных

технологий может стать мощным фактором дестабилизации международных отношений, подвергнуть серьёзному испытанию сложившуюся систему международных договоренностей по поддержанию

[1] Council of Europe. Convention on Cybercrime. – Budapest, 23.XI.2001; http://www.crime-research.org/library/cybercrime-convention.doc.

[2] http://www.usdoj.gov/criminal/cybercrime/roboslo.htm.

[3] *Лавров С.В.* Приветствие участникам научно-практической конференции «Наука, технологии и международные отношения в эпоху глобализации: роль образования и инноваций» – Москва, МГИМО, 24 апреля 2006 г.

стратегической стабильности (как на глобальном, так и на региональном уровне)»[1]. Применение информационных технологий в подобных (практически военных) целях фактически не регулируется международным правом.

Таким образом, быстрый прогресс в развитии информационных технологий приводит к возникновению новых существенных проблем в сфере международной безопасности и стабильности. По мнению ряда международных экспертов, проблемы безопасности занимают в круге проблем дальнейшего развития Интернета одно из центральных мест, а вопрос о контроле информационного пространства становится актуальным вопросом международной политики, который должен рассматриваться и решаться с участием всех заинтересованных сторон.

В России задачи по противодействию киберпреступности и кибертерроризму решаются в рамках утвержденной Президентом РФ доктрины информационной безопасности. В доктрине среди внешних источников угроз информационной безопасности РФ выделена деятельность международных террористических организаций.

В основных направлениях международного сотрудничества Российской Федерации в области обеспечения информационной безопасности выделено предотвращение несанкционированного доступа к конфиденциальной информации в международных банковских телекоммуникационных сетях и системах информационного обеспечения мировой торговли; к информации международных правоохранительных организаций, ведущих борьбу с транснациональной организованной преступностью, международным терроризмом и распространением наркотиков и психотропных веществ, незаконной торговлей оружием и расщепляющимися материалами, а также торговлей людьми.

Правовые нормы РФ в этой области ограничиваются Уголовным кодексом (специального закона пока нет). В Уголовном кодексе России понятие «терроризм» квалифицируется как «устрашение населения».

Весьма актуальной является в России проблема правовой ответственности за кражу информации из ведомственных баз данных. В ноябре 2005 г. Государственная Дума РФ ратифицировала Конвенцию Совета Европы «О защите физических лиц при автоматизированной обработке персональных данных» и приняла (в первом чтении) соответствующий законопроект «О персональных данных».

Одно из важных последствий теракта 11 сентября заключается в ужесточении западного законодательства в области криптографической защиты. Как отмечается в западной прессе, правительство США планирует разработать законодательные акты, которые запретят использование не сертифицированных в соответствующих ведомствах средствах шифрования. Российскому потребителю эта ситуация знакома: с 3 апреля 1995 г. в Российской Федерации был издан президентский указ №334, в котором, в частности, сказано: «В интересах информационной безопасности Российской Федерации и усиления борьбы с организованной преступностью запретить деятельность юридических и физических лиц, связанную с разработкой, производством, реализацией и эксплуатацией шифровальных средств, а также защищенных технических средств хранения, обработки и передачи информации»[2].[40].

В качестве рекомендаций, направленных на противодействие опасным тенденциям и повышение эффективности борьбы с кибертерроризмом, предлагаем следующее:

1. Организация эффективного сотрудничества с иностранными государствами, их правоохранительными органами и специальными службами, а также международными организациями, в задачу которых входит борьба с кибертерроризмом и транснациональной компьютерной преступностью.

2. международного взаимодействия по оказанию помощи при реагировании на транснациональные компьютерные инциденты.

3. Расширение трансграничного сотрудничества в сфере правовой помощи в деле борьбы с компьютерной преступностью и кибертерроризмом.

4. Принятие законов об электронной безопасности в соответствии с действующими международными стандартами и Конвенцией Совета Европы о борьбе с киберпреступностью.

ТЕРРОР В КИБЕРПРОСТРАНСТВЕ – МИФ ИЛИ РЕАЛЬНОСТЬ

А.И. Горев, (Омская академия МВД России)

Терроризм как сложное, многоаспектное и крайне негативное социально-политическое явление давно превратился в масштабную угрозу для безопасности всего человечества. Серьезную опасность для всего мирового сообщества представляет все более распространяющийся технологический терроризм, составной частью которого является информационный и кибернетический терроризм. Некоторые авторы отождествляют эти понятия, однако не следует смешивать информационный терроризм с терроризмом в сфере использования информационных систем. Нельзя также объединять эту дефиницию с терроризмом, использующим современные информационные технологии для достижения свих целей. В рамках данной статьи мы не будем рассматривать такие акции, как взрыв бомбы в пассажирском железнодорожном составе в Испании,

[1] *Крутских А.В*. Война или мир: международные аспекты информационной безопасности; Крутских А.В., Сафронова И.Л. Международное сотрудничество в области информационной безопасности // В сб.: Научные и методологические проблемы информационной безопасности. – М., МЦНМО, 2004.

[2] *Лукацкий А*. Безопасность сетей: Кибертерроризм: За и Против. – Компьютер-Пресс, №11 , 2001.

осуществленном дистанционной командой с использованием сотового телефона.

Отличительной чертой кибертерроризма является воздействие с удаленного расстояния на электронные системы государственного, экономического и военного управления с целью парализации их; вывод из строя важнейших объектов промышленности, связи, энергетики, транспорта, коммунального хозяйства, экологического контроля. Используемое оружие – вредоносные программные воздействия (вирусы, троянские программы и др.), программные закладки (логические бомбы и др.), активируемые в нужный момент времени или внедряемые в автоматизированные системы управления (далее – АСУ) с использованием информационных сетей (в частности – Интернет); генераторы электромагнитных импульсов для разрушения программного обеспечения и уничтожения баз данных защищенных компьютерных систем. По оценкам специалистов соотношение стоимости составляющих информационных систем – аппаратного, программного и информационного обеспечения, составляет 5 % : 25 % : 70 % всей системы. Объектами воздействия являются пункты управления стратегическими силами, атомные электростанции, аэропорты, системы жизнеобеспечения и др.

Отдельные специалисты в области компьютерной безопасности утверждают о надуманности угрозы компьютерного террора и принципиальной невозможности умышленного вредного воздействия на «жизненно важные сферы деятельности государства». Так, 12 ноября 2003 г. в Сиднее на конференции Gartner Symposium and IT Expo директор аналитической компании Gartner по информационной безопасности и рискам Р. Могулл заявил, что «несмотря на заметный процент широкомасштабных цифровых атак, кибертерроризм – это явление, с которым пока не приходилось сталкиваться на практике. Цель терроризма – изменить общество с помощью силы или насилия, которые порождают страх. Я хочу отставить в сторону само понятие кибертерроризма. Это теория, а не факт»[1].

Позже несколько информационных агентств, ссылаясь на Reuters, опубликовали информацию о прошедшей 16 апреля 2008 г. в Лондоне международной встречи специалистов по безопасности, на которой обсуждались вопросы объединения усилий по противодействию компьютерным угрозам. Итогом встречи явилось согласованное мнение о том, что «относиться к термину “кибертерроризм” серьезно нельзя»[2].

Развернутое обоснование этой позиции было изложено А. Астаховым[3], который провел детальный анализ информации об инцидентах с использованием вычислительной техники. Для подтверждения позиции «самые серьезные кибератаки по своим последствиям далеки от сценариев массовых разрушений» автор ссылается на результаты учений под кодовым названием «Цифровой Перл-Харбор», проведенных Военно-морским колледжем США совместно с компанией Gartner. В этих учениях эксперты, играющие роль кибертеррористов, имитировали широкомасштабную кибератаку на национальную сетевую инфраструктуру. По результатам учений был сделан вывод, что подобная кибератака действительно может вывести из строя системы телекоммуникаций в густо населенных районах, однако она не приведет к гибели людей или другим катастрофическим последствиям. Вывод А. Астахова сводится к тому, что «наиболее уязвимой к кибератакам является инфраструктура самой Сети, а понятие кибертерроризма часто используется для политических спекуляций и влияния на общественное мнение».

Аналогичного мнения придерживается эксперт в области программирования А. Коростылев: «реальных данных о том, что хакерам-террористам где-то действительно удалось осуществить глубокое и деструктивное проникновение в систему жизнеобеспечения государства, нет. Практически все случаи, которые можно отнести к кибертерроризму, связаны с уничтожением информационных сайтов политических противников, дестабилизацией работы гражданских серверов – опять же информационного назначения. На мой взгляд, кибертерроризм возможен пока лишь в рамках самой сети, без последствий для… “реальной жизни”»[4].

А. Солдатов также считает, что «эта опасность от террористов грозит нам меньше всего. Тому есть несколько причин:

1. Во многих российских стратегических объектах компьютеры, подключенные к внутренней сети, отделены от компьютеров с доступом в Интернет.

2. У террористов (как в России, так и за рубежом) нет хакеров такого уровня.

3. Террористы используют интернет не для взлома, а для пропаганды и коммуникации»[5].

Противоположные результаты приводит О. Нечипоренко, ссылаясь на военное руководство США, которое в 1997 г. смоделировало информационную атаку на важнейшие системы жизнеобеспечения страны с помощью независимых хакеров, общедоступных компьютерных программ и Интернет. В ходе эксперимента три хакера порознь на катерах в океане, снабженные портативными компьютерами и каналами спутниковой связи, доказали, что способны нанести государству вред, сравнимый с последствиями ядерного удара. Если бы атака была реальной, то в первый же день погибло не менее 20 тысяч человек, а экономические потери

[1] Gartner развенчал миф о кибертерроризме. // http://www.cnews.ru/news/top/index.shtml? 2003/11/13/151611.

[2] Эксперты по безопасности: «кибертерроризм» – это миф. // http://www.gazeta.ru/_techzone/2008/04/17_n_2697805.shtml; http://www.securitylab.ru/news/351684.php; http:// www.it-avenue.ru/news-new-3630.html и др.

[3] Астахов А.Реалии и мифы кибертерроризма. http://www.osp.ru/os/2003/05/183045.

[4] Гаврилов В. Реальная война в виртуальном мире. // «Труд» – 2005. – 1 сент.; http://www.trud.ru/article/01-09-2005/92921_realnaja_vojna_v_virtualnom_mire.html

[5] Солдатов А. Кибер террор: оценка уровня угрозы. Выступление на международной конференции «Правовое поле информационной безопасности: от данных к знанию, к уверенности через доказательство» 14-15 октября 2007 г. / Исследовательский центр Agentura.Ru // http://www.agentura.ru/equipment/psih/info/conferencepole/soldatov

составили несколько миллиардов долларов[1].

Данные по преступлениям в сфере компьютерной информации также весьма противоречива. По заявлению Н. Патрушева в 2005 г. сотрудники ФСБ отразили более миллиона компьютерных атак на информационные ресурсы федеральных органов госвласти, в том числе более 170 тыс. – на сайт президента РФ[2]. При этом по данным МВД России в последнее время ежегодно фиксируется около 18 тыс. преступлений в этой сфере. Несоответствие этих данных поднимает вопрос об активном противодействии злоумышленникам, осуществляющим кибератаки.

Находясь под воздействием этих противоречивых информационных потоков, обыватель должен задуматься над дилеммой о достоверности одной из точек зрения, о существовании опасности кибертерроризма и ее обоснованности. Прежде чем рассматривать возможные кибертеррористические операции, оценивать вероятность их осуществления и возможный ущерб и последствия, необходимо произвести их классификацию по направленности воздействия.

Исходя из определений применяемого оружия кибертерроризма, можно выделить два метода влияния: физическое, с использованием технологического оборудования, и программное, с использованием вредоносных программ и программных закладок (логических бомб). Вторая классификация может быть предложена по объекту воздействия, в качестве которого могут выступать:

– системы контроля и сбора данных (Supervisory Control and Data Acquisition – SCADA);

– автоматизированные системы управления технологическими процессами (далее – АСУ-ТП);

– автоматизированные системы управления локальными системами;

– базы данных справочно-информационных систем.

Использование технологического оборудования для разрушения программного обеспечения и уничтожения баз данных защищенных компьютерных систем. В сфере бизнеса одним из первых примеров кибертеррористического воздействия является взрыв кустарного электронного фугаса в подземном гараже международного бизнес-центра в Нью-Йорке, осуществленный в середине 90-х годов. Основной ущерб был причинен не разрушениями и человеческими жертвами, а несколькими днями простоя всех офисов бизнес-центра. Прямые убытки частных компаний и правительства США оценивались в сотни миллионов долларов, а непрямые, то есть связанные с нарушением ритма работы бизнес-центра и выходящих на него субъектов деловой жизни планеты, не поддаются исчислению. При этом совершенно не пострадали люди и технические средства офисов (компьютеры, факсы, модемы, ксероксы и т.п., стоимость которых составляет менее 10% стоимости всей системы обработки информации). Основной ущерб определялся потерей содержания информационных систем – программного обеспечения (часто уникального) и информации баз данных[3].

Электронные носители информации чувствительны к жесткому излучению. Например, информацию, записанную на магнитные носители можно модифицировать или уничтожить излучением радиопередатчика, электромагнитным полем электронно-лучевой трубки телевизора или мощной акустической системы. Мощное сверхвысокочастотное излучение выводит из строя микроэлектронные приборы и аппаратуру.

Данное направление является перспективным для развития, однако требует использования специального технологического оборудования, разработка и использования которого легко обнаруживается и может быть предотвращено. Исследование этой темы выходит за рамки данной статьи, посвященной рассмотрению программных воздействий.

Программный метод влияния может нанести большой ущерб при сокрытии источника воздействия. Более того, программируемое воздействие может быть спланировано на заранее определенную дату и время, создавая алиби злоумышленнику. Проведенное анкетирование показало, что менее 3 % пользователей персональных компьютеров берутся различить по последствиям после предварительной экспертизы следующие виды воздействий:

– вредоносные программы;

– действия инсайдера-злоумышленника;

– сбой системного или прикладного программного обеспечения;

– сбой аппаратного обеспечения.

Но даже эта малая доля пользователей не гарантирует достоверных результатов своих исследований. Можно констатировать, что широкое распространение вычислительной техники при невысоком уровне компьютерной грамотности и, одновременно – самоуверенности в обратном, породило серьезную проблему информационного общества – уязвимость личности, общества, государства от действий квалифицированного злоумышленника. Использование вредоносных программ и программных закладок (логических бомб) следует рассматривать относительно объектов воздействия, поскольку построение кибератаки существенным образом зависит от вида объекта и преследуемых целей. Для понимания конкретных особенностей атак воспользуемся второй классификацией и рассмотрим, насколько это возможно, объекты воздействия.

Воздействие на системы контроля и сбора данных (далее – SCADA-системы). Возможность построения и эксплуатации защищенных АСУ обсуждается постоянно. В настоящее время многие предприятия и компании управляют своими технологическими процессами при помощи систем контроля и сбора данных,

[1] Гаврилов В. Указ.соч.

[2] Солдатов А. Указ.соч.

[3] Дзлиев М. Общество и насилие: от «традиционного» терроризма к информационному // kcnti.csti.ru

уязвимость которых признается многими экспертами. Так, С. Макклу, президент известной на рынке информационной безопасности компании Foundstone, оценивает сложность осуществления атаки на SCADA-системы на 4-5 бала по 10-бальной шкале[1], обосновывая свое мнение тем, что, при отсутствии соответствующего регулирования со стороны государства, частные компании предпочитают экономить на безопасности. Кроме того, многие SCADA-системы функционируют в реальном времени и требования безопасности идут вразрез с требованиями производительности[2].

Аудит крупнейших американских промышленных предприятий специалистами компании Riptech, позволил сделать вывод об «уязвимости критичных для американской экономики SCADA-систем»[3]. Среди администраторов данных систем существует типичные заблуждения, препятствующих достижению адекватного уровня защищенности.

1. «SCADA-система размещается в физически изолированной сети». Действительно, SCADA-системы изначально создаются на базе физически изолированных компьютерных сетей, а их защита строится исходя из этого предположения. Этот фактор и определяет их незащищенность. Часто, для повышения эффективности управления подобными системами администратор, обеспечивающий функционирование операционной системы и сетевого взаимодействия, создает соединения между SCADA-системой и корпоративной сетью. Более того, для оперативности принятия решений и выполнения собственных функциональных обязанностей, связанных с бесперебойной работой информационной системы, администратор устанавливает защищенное соединение с Internet. В качестве каналов доступа могут использоваться соединения по каналам сотовой телефонии и Wi-Fi[4].

2. «Существующие соединения между SCADA-системой и корпоративной сетью надежно защищены при помощи средств контроля межсетевого доступа». На практике в большинстве SCADA систем существуют точки входа из корпоративной сети, незащищенные межсетевыми экранами и системами выявления атак, а некоторые из них могут быть вообще никак не защищены.

Примером является авария одного из основных поставщиков австралийской энергосистемы компании Integral Energy после заражения Windows-терминалов, используемых в качестве консоли мониторинга и удаленного управления, вирусом W32.Virut.CF в октябре 2009 г. Обследование компании показало отсутствие разграничения между сетью общего пользования и сетью контроля электротехнического оборудования[5].

3. «Для управления SCADA-системой требуются узкоспециализированные знания, что делает задачу получения удаленного контроля над подобной системой для хакера чрезвычайно сложной». Предполагается, что у злоумышленника отсутствует «инсайдерская» информация об архитектуре и средствах управления SCADA-системой. Действительно, системы используют специализированное программное обеспечение, ориентированное только на выполнение поставленной задачи. Однако подобная программа вместе с технической документацией на нее может использоваться аналогичным предприятием. Если в качестве атакующего выступает бывший сотрудник предприятия или компании-разработчика системы, то это предположение нельзя считать корректным[6].

В качестве примера можно привести осуществить спуск загрязненной воды в водопроводы в Австралии в ноябре 2001 г. Некто В. Боуден был осужден на два года лишения свободы за использование Internet, беспроводного радио и хищения управляющего программного обеспечения для осуществления слива загрязненной воды в реку у побережья Маручидора (Квинсленд). Боуден работал консультантом в водном проекте и совершил преступление после получения отказа в работе на полную ставку. Он 45 раз пытался получить доступ к системе водоочистки.

4. В дополнение к проблемам, указанным специалистами компании Riptech, следует отметить заблуждение, вызванное самоуверенностью администраторов систем. Считая отсутствие открытой информации о дистанционном управлении системой достаточно надежной защитой от злоумышленника, они не предпринимают дополнительных действий для фиксации попыток несанкционированного доступа и вычисления адреса атакующего. В приведенном ранее примере деяния злоумышленника стали возможны только после 45 (!) неудачных попыток.

Воздействие на АСУ-ТП. В отличии от SCADA-систем, рассмотренных ранее, АСУ-ТП имеют функции управления техническими процессами в автоматизированном (с участием оператора) и автоматическом (без участия оператора) режимах. В ряде случаев это обусловлено монотонностью операций, что делает их легко алгоритмизируемыми и привлекательными для автоматического управления (например – подача деталей на конвейер). Другая категория – управление быстро меняющимися процессами, отслеживать которые человек-оператор не успевает. Считается, что замкнутость данных систем, специализированное программное обеспечение и отсутствие легального дистанционного управления делает невозможным проведение кибератаки.

[1] Vamosi R. Cyberterrorists don't care about your PC. ZDNet Reviews, 2002, July 10.
[2] National Strategy to Secure Cyberspace, Draft, 2002 September. Цитируется по Астахов А. Указ.соч.
[3] Understanding SCADA system security vulnerabilities, Riptech, Inc. 2001 January.
[4] Данная информация получена интервьюированием администраторов информационных систем. Для выполнения должностных обязанностей, немедленного восстановления работоспособности системы при сбоях или выходе ее из строя по каким-либо причинам в любое время (и даже в отпуске), администраторы организуют каналы доступа, известные только им.
[5] Энергосистема Австралии спасена благодаря Linux // http://www.securitylab.ru/news/ 386273.php. – 2009. – 6 окт.
[6] Vamosi R. Указ.соч.

Однако подобные системы слабо защищены от действий инсайдера-злоумышленника. Примером может служить остановка главного конвейера Волжского автозавода в г. Тольятти в 1983 г., произошедшая после внесения программистом программы-счетчика подаваемых на конвейер деталей. «Логическая бомба», сработавшая после обнуления счетчика, нарушила ритм работы конвейера и нанесла ущерб более 1 млн.руб.[1]

В 2008 г. организация Secure Computing опубликовала результаты опроса 199 экспертов в области сетевой безопасности, проведенного в США, Канаде и Европе. 62 % североамериканских специалистов признали, что их сети напрямую подключены к другим IP-сетям или к Интернет. Более 50% респондентов охарактеризовали степень защищенности газодобывающих, нефтяных, химических, телекоммуникационных, транспортных компаний, служб жизнеобеспечения, сервиса и почты как не готовых противостоять серьезным компьютерным атакам. Наиболее уязвимой и значимой отраслью для атак кибертеррористов эксперты назвали энергетику: она является наиболее желанной целью для хакеров (33%), наиболее уязвимой (30%) и последствия атаки на нее будут наиболее серьезными (42%)[2]. Так, массовые перебои с энергоснабжением в Бразилии в сентябре 2007 г., когда без света остались более 3 млн. жителей в нескольких десятках городов, были вызваны манипулированием системами управления. Исследования, проведенные Департаментом энергетики США в лаборатории Idaho National Labs показали, что каскадное отключение подсистем реально осуществимо[3].

В случае если объектом воздействия станет химическое производство, последствия будут сравнимы только с результатами действия химического оружия. Б. Мыльников считает самыми опасными видами терроризма ядерный и кибертерроризм. Для подтверждения своей позиции он ссылается на внедрении злоумышленниками в компьютер Игналинской АЭС в Литве вируса, в результате чего могла произойти авария, подобная чернобыльской. Известны также случаи проникновения в мае 1998 г. хакера из США в компьютерную сеть ядерного исследовательского центра Bhabha Atomic research center, занимавшегося разработкой атомного оружия. В 1999 г. израильская исследовательская группа Siri Security research исследовала 36 млн. интернет-адресов в 214 странах и нашли свыше 730 тысяч уязвимых мест, в том числе в информационных системах ядерных исследовательских центров США, Индии и Франции[4].

Воздействие на локальные АСУ подвижных объектов. В отличие от ранее рассмотренных АСУ-ТП, локальные АСУ подвижных объектов предназначены для управления и контроля ограниченными пространственными системами, функционально не имеющими статического дистанционного управления. В настоящее время локальные АСУ распространены чрезвычайно широко. К ним в первую очередь можно отнести системы управления подвижными объектами – самолетами, поездами, автомобилями и др. Возможность дистанционного воздействия на объекты этого рода рассматривалась давно, однако только сейчас, с появлением и всепроникающим распространением систем связи и миниатюризацией вычислительной техники, появился реальный потенциал их распространения.

Например, в Великобритании прошла испытания и готовится к внедрению национальная система сплошного, непрерывного и всеобъемлющего контроля скоростного режима всех автотранспортных средств – Intelligent Speed Adaptation (ISA). Система ISA, предполагает внедрение в контур управления скоростью автомобиля узла, контролирующего его реальную скорость и препятствующего ее выходу за определенные для данного географического района пределы. Это устройство, жестко ограничивающее скорость автомобиля, либо предупреждающее водителя о нарушении скоростных ограничений, может быть основано на использовании системы GPS[5].

Более сложные системы дистанционного управления автопилотами преследуют цели противодействия угонам самолетов для последующего проведения террористических актов. В 2006 г. концерн Airbus объявил о масштабной программе по созданию автоматической защиты от угона самолетов. Разработки ведутся совместно с Siemens и специалистами из Технического университета Мюнхена. В 2007 г. компания Boeing представила систему автоматического управления самолетами, которая позволяет управлять лайнером с земли. Автопилот полностью защищен от постороннего вмешательства. При потенциальной опасности пилоты имеют возможность вручную активировать автопилот и передать управление самолетом наземным службам. Автопилот может включиться сам при срабатывании датчиков давления, вмонтированных в дверь кабины, после чего механизм невозможно будет отключить вплоть до посадки[6].

Аналогичные системы разрабатываются и в России. Основанная на принципах автопилота спецаппаратура, установленная на самолет, в том числе на гражданский лайнер, позволяет управлять воздушным судном с земли без участия экипажа. После поступления по радиолинии на борт самолета команды автопилот устанавливает определенное положение рулей так, что изменить их невозможно. Это позволит вывести воздушное судно в заданный район и поставить его, к примеру, в круговой вираж[7].

---

[1] Згадзай О.Э., Казанцев С.Я., Филиппов А.В. Информатика и математика. М.: ИМЦ ГУК МВД России. – 2002. – С. 305.

[2] Secure Computing: Энергетика наиболее уязвима для атак кибертеррористов. // http://www.securitylab.ru/news/362956.php. – 2008. – 13 нояб.

[3] Хакеры оставили без электричества 3 млн бразильцев. // http://www.securitylab.ru/ news/387521.php. – 2009. – 10 нояб.

[4] Глава АТЦ: самые опасные виды терроризма – ядерный и кибертерроризм. // http://www.securitylab.ru/news/ 274644.php. – 2006. – 28 сент.

[5] Vehicle speed-limiter systems loom http://www.channel4.com/news/articles/science_ technology/vehicle+speedlimiter+ systems+loom/2454242. – 2008. – 15 сент.

[6] Автопилот от Boeing террористам не сдается http://www.vokrugsveta.ru/news/400/ – 2007. – 12 март.

[7] Бывший главком ВВС генерал армии А Корнуков утверждает, что Россия располагает техническими средствами,

Однако рассматривая подобные системы, следует понимать ограничение их применения и уязвимость. В 2009 г. аэробус «Эр Франс», совершавший рейс по маршруту Рио-де-Жанейро – Париж, потерпел катастрофу над Атлантическим океаном. Согласно выводам комиссии, на самолете отказали автопилот, система автоматической подгазовки и датчики скорости. Компьютерная система Air Data Inertial Reference Unit (ADIRU), которой оснащаются современные пассажирские лайнеры, отвечает за передачу информации, включая высоту полета и скорость ветра, на альтиметры в кабине пилотов, информационные дисплеи и автопилот. По заявлению руководителя экспертной группы А. Буйара, при получении с датчиков скорости противоречивых данных система автопилотирования «перестает функционировать в нормальном режиме»[1].

ADIRU уже становилась причинной опасного поведения воздушных судов. В 2008 г. сбой в системе привел к травмам пассажиров аэробуса А330 австралийской авиакомпании Qantas Airways. При включенном автопилоте самолет начал рывками терять высоту, пока пилоты не перешли на ручное управление. По официальному заявлению Австралийского бюро транспортной безопасности «в течение примерно двух минут после сбоя (система ADIRU) генерировала случайные и неправильные величины для формирования угла атаки самолета[2].

И хотя в приведенных конкретных случаях не возникала проблема теракта, закономерно возникновение вопроса о возможной модификации программы автопилотов, тем более, что такой потенциал заложен изначально[3]. Следует также вспомнить, что одной из версий теракта 11 сентября в Нью-Йорке являлось использование автопилотов в самолетах, таранивших башни бизнес-центра. Действительно, террористам, имевшим несколько часов полетной практики на легкомоторном самолете затруднительно (если вообще возможно) вывести на большой скорости тяжелый аэробус точно в цель. Программа автопилота может выполнить эту задачу значительно лучше.

Наличие уязвимостей или недокументированных функций в программном обеспечении делает чувствительным и ненадежным любое оборудование. Так, во время войны в Персидском заливе компьютерная система управления бортовыми системами самолетов «Мираж» была отключена кодовым сигналом[4].

Воздействие на локальные АСУ стационарных объектов. В данном классе систем следует рассматривать современные системы управления, не связанные с технологическими процессами. К таким в первую очередь следует отнести комплексы «умный дом», находящие все большее распространение во всем мире. Востребованность данной разработки можно определить тем, что по запросу поисковая система Яндекс выделила 28 млн.стр. В современном понимании умный дом – единая система управления в совмещающая в себе следующие системы:

– восприятия различных параметров окружающей среды: влажность воздуха, освещенность, температура, качество воздуха, давление, возникновение протечек воды и утечек газа, присутствие человека;

– управляющие элементы освещением, бытовой техникой, воротами и рольставнями, водоснабжением и канализацией, вентиляцией и отоплением;

– устройства обратной связи, начиная от кнопок, выключателей и светодиодных индикаторов до возможности управления, используя все современные способы и протоколы проводной и беспроводной связи: пульты дистанционного управления, беспроводные панели, мобильные телефоны и карманные компьютеры. Ряд систем допускают управление голосом.

Но главной составляющей умного дома является центр обработки информации и управления. Умный дом может быть запрограммирован на выполнение определенных задач, называемых сценариями: от простых реакций на воздействия, например включение обогревателя при определенном уровне температуры в помещении, до сложного комплексного управления, например одновременное закрытие жалюзи, плавное выключение света, включение телевизора и DVD плеера на определенный фильм одной голосовой командой[5].

Все технологии и системы, используемые в России, разработаны и производятся в Европе, США и Китае. Разнообразие производителей определяет наличие и доступность стандартизированных протоколов взаимодействия систем управления «умным домом» с использованием проводной и беспроводной связи. Это, в свою очередь, актуализирует вопросы защиты людей в подобных сооружениях: легко представить негативные последствия распыления аэрозоля в системе вентиляции и кондиционирования при закрытых рольставнях, вышедшею из-под управления бытовую технику и освещение, создающие эффект присутствия постороннего в «умном домом». Подобное воздействие «умного дома» на его обитателей укладывается в определение терроризма, предложенное профессором Ю.М. Антоняном: «терроризм – это насилие, содержащее в себе угрозу другого, не менее жестокого насилия, для того, чтобы вызвать панику, нарушить и даже разрушить государственный и общественный порядок, внушить страх, заставить противника принять желаемое решение,

---

способными предотвратить атаки террористов с применением воздушных судов. См.: И Плугатарёв Самолет с террористами условно сбит... // Газета «Независимое военное обозрение». – 2006. – 1 сент. См.: http://nvo.ng.ru/ forces/2006-09-01/1_interceptor.html.

1 Шестаков Е. Смертельные самолеты «Эр Франс» http://www.rg.ru/2009/07/14/samolet-site.html – 14 июля 2009 г.

2 Эксперты свалили вину за крушение А330 на компьютер // http://www.rosbalt.ru/ 2009/06/06/646074.html.

3 В требованиях к конкурсантам на должность пилотов в качестве обязательных умений и навыков фигурирует перепрограммирование автопилота.

4 Згадзай О.Э., Казанцев С.Я., Филиппов А.В. Указ.соч. – С. 302.

5 Что такое умный дом? // http://www.greenvision.ru/?do=menu&id=17857

вызвать политические и иные изменения. По-видимому, это – устрашение смертью»[1].

Воздействие на базы данных справочно-информационных систем является одним из легко осуществимых деяний, имеющих серьезные последствия. В качестве примера можно рассматривать сбои, происходящие на фондовых биржах. В декабре 2005 г. на Токийской фондовой бирже брокер банка Mizuho Financial совершил ошибку и вместо одной акции J-Com по цене 610 тыс. йен (более $ 5000) предложил участникам рынка купить 610 тысяч акций по цене одной йены (0,8 цента). В результате предложение ценных бумаг J-Com на рынке в 41 раз превосходило реальное количество акций, выставленных на продажу. Банк потерял 225 млн. долларов, а биржа утратила доверие инвесторов[2]. Данная ситуация стала возможной вследствие отсутствия проверки вводимых брокерами данных. Она наглядно демонстрирует вероятность негативных последствий воздействия вредной информации для финансового сектора, и легкость, с которой данная операция может быть произведена. Потери сотен миллионов долларов могут иметь катастрофические последствия для экономики многих стран.

Информационные системы, обрабатывающие информацию ограниченного доступа, как правило, имеют защиту от проникновения извне. Однако локальная сеть, связывающая отдельные рабочие места, и сами компьютеры часто оказываются незащищенными от злоумышленных действий. В настоящее время в России в соответствии с Указом Президента от 17 марта 2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена» локальные сети государственных органов должны строиться замкнуто и не иметь свободного доступа к Интернет. Однако использование стандартного программного обеспечения и доступность технических средств связи существенным образом осложняет эту задачу. Уже зарегистрированы случаи подключения к Интернет из локальных сетей с использованием радиомодемов сотовых сетей связи[3]. Включение радиомодема в USB-разъем персонального компьютера и последующее подключение к Интернет без программ антивирусной защиты приводит к проникновению в информационную сеть вредоносных программ. Это, в свою очередь, является причиной возникновения риска уничтожения или распространения информации ограниченного доступа.

Рассмотренные примеры кибервоздействия на автоматизированные системы управления и обработки информации наглядно демонстрируют несостоятельность утверждения об отсутствии кибертеррористической угрозы. Современное информационное общество в повседневной жизни стало зависимым от нормального функционирования компьютеризированных систем. А программное обеспечение этих систем уязвимо к дистанционному управлению. Это, в свою очередь, определяет необходимость защиты от потенциальных угроз.

Для защиты критически важных систем управления и обработки информации следует:

– проводить регулярный аудит уязвимостей сетевых систем автоматики и контроля;

– производить обмен информацией по уязвимостям и атакам на них;

– предоставлять информацию о кибератаках правоохранительным органам. Каждый факт неправомерного доступа или безуспешной попытки доступа должен быть расследован, а злоумышленник – установлен и наказан.

О СИСТЕМНОМ ПОДХОДЕ ПРИ ДАЛЬНЕЙШЕМ РАЗВИТИИИ В СУБЪЕКТАХ РОССИЙСКОЙ ФЕДЕРАЦИИ АПК «БЕЗОПАСНЫЙ ГОРОД» С ЦЕЛЬЮ ОБЕСПЕЧЕНИЯ КОМПЛЕКСНОЙ БЕЗОПАСНОСТИ В РЕГИОНЕ

Д.Ю. Солоненко (ГУВД по г. Москве)

Глобализация и активное развитие инфраструктуры населенных пунктов, увеличивающиеся миграционные потоки и как следствие, рост потенциальных криминогенных угроз требует новых подходов и решений для обеспечения безопасности и правопорядка. В немалой степени поиск новых форм и методов защиты населения обуславливает развитие информационно-телекоммуникационных технологий, а также систем связи и объективного контроля, позволяющих создавать комплексные системы безопасности населенных пунктов.

В настоящее время в субъектах Российской Федерации создаются и внедряются правоохранительные сегменты аппаратно-программных комплексов (АПК) «Безопасный город» (в городе Москве – система обеспечения безопасности города (СОБГ).

Совершенные в последнее время террористические акты на территории Российской Федерации свидетельствуют о необходимости пересмотра общего подхода к обеспечению комплексной безопасности на всех наиболее важных объектах городской инфраструктуры и в местах с массовым пребыванием людей.

Указ Президента Российской Федерации от 31 марта 2010 г. № 403 «О создании комплексной системы обеспечения безопасности населения на транспорте» и принятые решения на совещании в г. Кизляре требуют от органов исполнительной власти и правоохранительных органов согласованных действий и выработки

[1] Антонян Ю.М. Терроризм: криминологическое и уголовно-правовое исследование. М., 1998 г. С. 10.

[2] http://www.banki.ru/news/bankpress/?ID=110363. – 2005. – 12 дек.

[3] Данные получены интервьюированием слушателей факультета повышения квалификации. Как правило, инсайдер не имел злого умысла, но недостаточная грамотность в области информационных технологий не позволила предвидеть последствия деяний.

комплекса мер по предотвращению террористических актов, включая дальнейшее развитие АПК «Безопасный город» (СОБГ).

Дальнейшее развитие АПК «Безопасный город» (СОБГ) в субъектах Российской Федерации также предусмотрено протоколом заседания Национального антитеррористического комитета (НАК) от 8.12.2009 г. № 22дсп и планом реализации Стратегии развития информационного общества Российской Федерации до 2011 года, утвержденным решением заседания Совета при Президенте Российской Федерации по развитию информационного общества Российской Федерации от 23.12.2009 г.

Указанными документами определена приоритетная задача – обеспечить системный подход при развитии АПК «Безопасный город» (СОБГ), с проведением следующих мероприятий:

создание и внедрение информационно-аналитической системы «Безопасный город» (п. 4.8. плана реализации Стратегии);

внедрение средств автоматической видеофиксации нарушений Правил дорожного движения (п. 4.12 плана реализации Стратегии);

создание системы обеспечения вызова экстренных оперативных служб через единый номер «112» (п. 4.18 плана реализации Стратегии);

внедрение навигационно-мониторинговых систем ГЛОНАСС в органах внутренних дел Российской Федерации и внутренних войсках МВД России (п. 4.21 плана реализации Стратегии) и др.

оборудовать места массового пребывания людей инженерно-техническими средствами охраны, в том числе системами видеонаблюдения, сохранив объемы запланированного на 2010 год финансирования программ формирования АПК «Безопасный город», обеспечив при этом внедрение программно-аппаратных средств, совместимых (унифицированных) с техническими комплексами, применяемыми правоохранительными органами и спасательными подразделениями (раздел 1, п. 8 план-графика НАК) с целью использования циркулирующей в АПК «Безопасный город» (СОБГ) видеоинформации для дальнейшего проведения идентификационных исследований;

при развертывании аппаратно-программного комплекса «Безопасный город» проработать возможность сопряжения с АПК систем безопасности крупных объектов (вокзалы, метрополитены, стадионы, торговые и культурно-развлекательные центры), охранных организаций и служб безопасности (раздел 1, п. 8 план-графика НАК).

В настоящее время в Москве разработан алгоритм совместных действий всех взаимодействующих структур, который определен «Комплексной городской целевой программой профилактики правонарушений, борьбы с преступностью и обеспечения безопасности граждан на 2006-2010 годы» утвержденной Законом города Москвы от 19 апреля 2006 года № 16. Данной Программой и принятыми в последние годы решениями Антитеррористической комиссии города предусматривалось проведение мероприятий по интеграции систем видеонаблюдения различных городских объектов в СОБГ. Предлагалось на базе существующей информационно-телекоммуникационной инфраструктуры создать комплексную систему обеспечения безопасности Московского региона и включить в ее состав:

систему телевизионного наблюдения в подъездах многоквартирных домов жилого сектора города;

систему городского видеонаблюдения на объектах массового скопления людей;

системы видеонаблюдения, созданные органами исполнительной власти города на объектах подведомственных организаций;

систему видеонаблюдения ГУП «Московский метрополитен»;

системы управления дорожным движением и контроля за дорожной обстановкой ГИБДД «Старт» и «Каскад»;

системы видеонаблюдения ФСО России, ФСБ России, ГУ МЧС России по городу Москве, установленных на территории города Москвы;

общероссийскую комплексную систему информирования и оповещения населения (ОКСИОН);

интегрировать в КСОБН систему управления мобильными нарядами (СУМН) ГУВД) и др.

Учитывая, что председателем Правительственной комиссии по профилактике правонарушений – Министром внутренних дел Российской Федерации Р.Г. Нургалиевым в обзоре практики внедрения, эксплуатации и развития АПК «Безопасный город» в регионах Российской Федерации **с** положительной стороны отмечена проводимая всеми заинтересованными организациями города Москвы работа по обеспечению системного подхода по созданию, внедрению и эксплуатации всех компонентов АПК «Безопасный город» (системы видеонаблюдения, навигационно-мониторинговые системы органов внутренних дел, региональные сегменты ОКСИОН и др.) с целью обеспечения комплексной безопасности в регионе, ГУВД по г. Москве было выбрано в качестве пилотной зоны для тестирования аппаратно-программных комплексов по идентификации личности.

Во исполнение принятых НАК решений, в соответствии с распоряжением ГИАЦ МВД России, в подразделениях ГУВД по г. Москве проводится тестирование разработанных различными организациями систем интеллектуального видеоанализа, позволяющих в результате обработки видеопотока СОБГ создавать «архив видеоизображений» для последующего его использования в подразделениях ГУВД по г. Москве.

С января 2010 года в ГИАЦ МВД России, ЦОРИ КМ ГУВД и ЦОРИ КМ УВД по ЮАО проводится тестирование трех аппаратно-программных комплексов по идентификации личности (АПК «Сова» (версия 2.0), программные средства ЗАО «Диссо» и ЗАО «Техносервъ»).

В соответствии с требованиями ГИАЦ МВД России, в ходе проводимого тестирования по каждой системе оцениваются следующие показатели:

наличие программных средств, позволяющих улучшить качество получаемого с установленных систем телевизионного наблюдения видеосигнала, и эффективность их функционирования при обработке реального видеопотока;

создание в результате обработки видеопотока «архива видеоизображений» для последующего его использования в подразделениях ЦОРИ КМ.

В ходе тестирования проверяются оптические алгоритмы поиска по измерению (биометрии) характерных (реперных) точек сочленения основных костей черепа человек, позволяющих осуществлять идентификацию по: субъективным портретам, фотографиям (живых лиц, неопознанных трупов); по видеороликам (снимки с камер банкоматов, входных дверей жилых домов, прилегающих территорий к объектам массового посещения – магазины, развлекательные и спортивные центры).

Ориентировочный срок завершения тестирования – апрель-май т.г. В августе т.г. на заседании Научно-технического совета МВД России планируется утвердить результаты проведенного тестирования и принять решение о централизованных закупках, в рамках гособоронзаказа на 2011-2013 г.г., для всех органов внутренних дел одной из перечисленных систем. В подразделениях ЦОРИ КМ ГУВД будет установлено рабочее место системы, с которого в результате обработки поступающего видеопотока, независимо от ведомственной принадлежности систем видеонаблюдения, будет формироваться «архив видеоизображений» для последующего его использования в подразделениях ЦОРИ КМ ГУВД.

Вместе с проводимыми мероприятиями по внедрению систем интеллектуального видеоанализа актуальным является вопрос по созданию и внедрению программных средств, позволяющих автоматически распознавать типовые ситуации в поле обзора видеокамеры и передавать информацию в органы внутренних дел и другие организации для реагирования.

С целью выполнения принятых решений по обеспечению комплексной безопасности считается целесообразным:

Создание в субъектах Российской Федерации координирующего органа по исполнению плана реализации Стратегии и принятых на заседании НАК решений для взаимодействия с федеральными структурами, ответственными за выполнение указанных работ.

Определение государственных заказчиков на проведение мероприятий по обеспечению комплексной безопасности в субъекте Российской Федерации.

Определение должностных лиц, ответственных за разработку концепции, технико-экономического обоснования и технического задания по созданию, на базе существующей информационно-телекоммуникационной структуры, комплексной системы обеспечения безопасности в субъекте Российской Федерации.

Совместное использование единой картографической основы и баз данных по объектам города для обеспечения информационно-аналитической и технической поддержки управленческой деятельности руководства города Москвы, оперативных штабов по сбору, анализу, обработке и принятию решений, комплексному управлению всеми имеющимися в городе силами и средствами в особых условиях.

Определение перечня информации общего (коллективного) пользования, хранящейся в базах данных различных организаций, с последующим предоставлением доступа к ней всех заинтересованных пользователей, и регламент (порядок) актуализации информации коллективного пользования.

Создание реестра внедренных и создаваемых в регионе информационных ресурсов (автоматизированные системы, базы данных, межведомственные регламенты информационного взаимодействия, учебные и информационные пособия и др.) для организации доступа к нему заинтересованных организаций и ведомств, в том числе расположенных в субъектах Российской Федерации.

Достичь желаемого результата можно консолидацией усилий всех участников создания СОБГ и проведением жесткой централизованной единой технической политики.

АНАЛИЗ ЦЕЛЕСООБРАЗНОСТИ РАЗРАБОТКИ МОДЕЛЕЙ НАРУШИТЕЛЕЙ ПРИ ПОВЫШЕНИИ АНТИТЕРРОРИСТИЧЕСКОЙ УСТОЙЧИВОСТИ РАЗЛИЧНЫХ КАТЕГОРИЙ ОБЪЕКТОВ

С.Б. Ахлюстин (Воронежский институт МВД России)

Анализируя типовые требования по антитеррористической защищенности критически важных и потенциально опасных объектов, разработанные межведомственной рабочей группой (в состав которой входят также представители подразделений вневедомственной охраны), одним из важнейших аспектов обеспечения безопасности является использование технических средств охраны. Так как, охраняемые объекты указанной категории являются крупными, распределенными и часто находятся за пределами населенных пунктов, то есть находятся вне зоны действия пунктов централизованной охраны, следовательно, необходимо использовать такие системы охраны, которые обеспечивали бы не только всестороннюю безопасность, но и возможность удаленного мониторинга и, соответственно, быструю и качественную передачу данных на центральный диспетчерский пункт.

Рассмотрим организацию повышения антитеррористической защищенности объектов жизнеобеспечения с использованием интегрированных систем безопасности (Рис.1.).

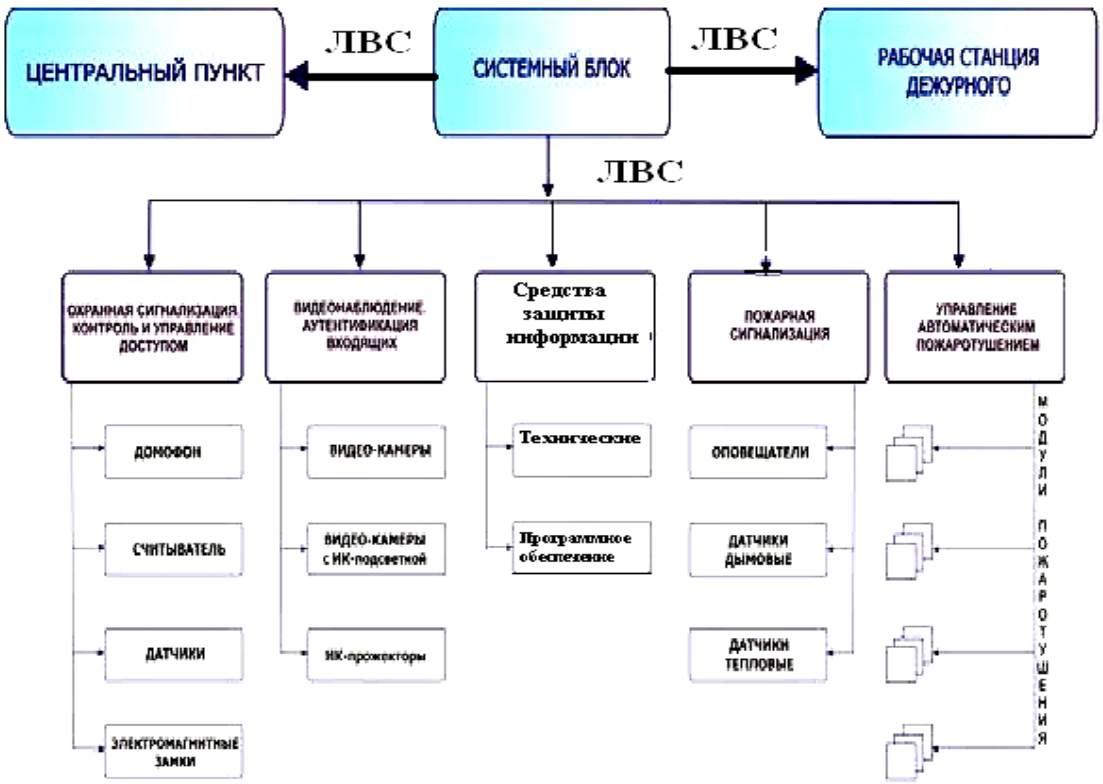

Рис. 1. Интегрированная система безопасности

1. Цели и задачи создания интегрированной системы безопасности

1.1. Объекты защиты

- люди (персонал предприятия и посетители);
- имущество:
  - здания и сооружения;
  - технологическое оборудование и приборы;
  - материальные и финансовые ценности;
  - готовая продукция;
  - интеллектуальная собственность (ноу-хау);
- конфиденциальная информация (на материальных носителях, а также циркулирующая во внутренних коммуникационных каналах связи и информации, в кабинетах руководства предприятия, на совещаниях и заседаниях).

1.2. Угрозы безопасности

- чрезвычайная ситуация: пожар, разрушение, авария, диверсия и т.п.;
- хищение или порча имущества;
- утечка конфиденциальной информации.

1.3. Категории нарушителей

- Внешние.
- Внутренние.

Внутренний нарушитель - это лицо или группа лиц, обладающих правом доступа на объект и к материальным ценностям в силу выполнения служебных или иных обязанностей, при этом внутренних нарушителей можно классифицировать тремя категориями:

- одиночный нарушитель - это лицо из числа персонала, имеющее определенные служебные или иные обязанности с ограниченным доступом и ограниченными возможностями хищений и порчи материальных ценностей, осуществляемых в мелких масштабах, но систематически с нарастанием массы нарушителей;

- неорганизованный групповой нарушитель - это группа лиц при наличии случайного "сговора" с представителем среднего звена руководства предприятия или охраны. Связи между членами группы неустойчивы, случайны, как правило, прекращаются после свершенного одного или нескольких преступлений;
- организованная преступная группировка - это группа лиц, как правило, включающая руководителей среднего и верхнего звена, получившая открытый доступ к материальным ценностям и имеющая постоянного лидера. Возможны масштабные регулярные хищения крупных партий материальных ценностей с использованием специальных каналов транспортировки, связи и фальсификации учетно-отчетной документации.

1.4. Задачи:

- противоаварийный и пожарный контроль;
- предотвращение несанкционированного проникновения на территорию предприятия;
- ограничение и контроль доступа персонала и посетителей;
- контроль доступа транспорта;
- коммерческий учет;
- автоматизированный учет рабочего времени;
- удаленный визуальный мониторинг;
- контроль действий персонала охраны;
- возможность передачи данных по различным каналам связи;
- управление системами жизнеобеспечения (системы пожаротушения, дымоудаления, эвакуации и т.д.).

Система должна контролировать реакцию сотрудников охраны, регистрировать их действия и осуществлять периодическую проверку его бдительности.

Смена сотрудников охраны фиксироваться вводом личного пароля, а также видеокамерами. Время начала и окончания работы дежурного охранника должно регистрироваться в базе данных системы. Во время обхода территории объекта дежурная охрана должна отмечаться в контрольных точках.

2. Организация интегрированной системы безопасности

Проектирование систем защиты периметров требует использования комплексного подхода. Применяемые средства и методы должны быть разумно достаточны, адекватны возможной угрозе, а меры противодействия должны быть сбалансированными, то есть распределены по возможности в соответствии с вероятностью угроз и важностью защищаемой зоны. Кроме того, устанавливаемые средства и системы не должны создавать препятствий для нормального функционирования объекта и тем более быть опасными для сотрудников или других людей, проходящих рядом с периметром. Структура комплекса безопасности включает в себя:

- периферийное оборудование (контроллеры, считыватели, охранные извещатели, видеокамеры, электромагнитные замки, турникеты, картоприемник, и т.п.);
- серверное оборудование подсистем охранной и пожарной сигнализации, видеонаблюдения, контроля доступа (на базе персональных компьютеров);
- удаленные рабочие места интегрированного комплекса безопасности и отдельных подсистем (охранная и пожарная сигнализация, видеонаблюдение, контроль доступа);
- локальная сеть системы безопасности, активное и пассивное сетевое оборудование.

Построение эквивалентной схемы надежности интегрированной системы безопасности (ИСБ) при проектировании и дальнейшей эксплуатации целесообразно начать с общего подхода к разработке моделей нарушителей, адекватно спроектировать необходимую систему защиты, а затем предметно оценить ее эффективность в плане устойчивости к воздействию факторов криминогенного характера.

Необходимость использования моделей во многом определяется трудностями натурных испытаний сложных систем. Более того, для целого ряда систем такие испытания вообще невозможны. Поэтому исследование эффективности ИСБ осуществляется с использованием различных моделей, в том числе моделей нарушителя.

Для широкого круга объектов (объектов потенциального воздействия нарушителей – ОПВН) для обеспечения их физической защиты важна разработка перечня потенциальных угроз и, прежде всего, проектной угрозы. Только она позволяет адекватно спроектировать необходимую ИСБ конкретного объекта, а затем и предметно оценить ее эффективность. Составным элементом проектной угрозы является проектная модель нарушителя (ПМН), поэтому формирование такой модели – актуальная задача.

Однако в отечественных и зарубежных методических и руководящих документах, касающихся анализа уязвимости объектов или оценки эффективности ИСБ четко не сформулированы ни цели для которых создаются модели нарушителя, ни методики создания самих моделей. В данной статье будет рассмотрена общая постановка задачи создания моделей нарушителей и состояние решения этой задачи за рубежом.

Отечественные руководящие документы указывают, что модель нарушителя должна формироваться и уточняться, исходя как из особенностей объекта и технологических операций, выполняемых на нем (стабильные факторы), так и изменяющихся факторов – социальных условий, складывающихся в районе расположения объекта и в самом коллективе предприятия, социально-психологических особенностей отдельных групп людей и личностей, а также обстановке в мире, стране, регионе и т.п. Таким образом, в одной

модели должны учитываться многообразные факторы, относящиеся к разным аспектам действительности, зачастую не связанные между собой. Это свидетельствует о том, что в модели с точки зрения системного подхода отсутствует учет принципа множественности описания сложных систем, а это приводит к сложностям в использовании моделей в работе.

Принцип множественности описания сложных систем предполагает, что ИСБ рассматривается с разных точек зрения, в различных целях, и она не может быть отображена одной какой-либо универсальной моделью.

Набор характеристик, описывающих данную модель, будет отличаться (зачастую значительно) от набора характеристик других моделей этой же системы. Именно вследствие того, что модели одной системы, созданные в различных целях, отличаются друг от друга, строить какую либо общую модель системы, описывающую все (или очень многие) свойства, как правило, нецелесообразно. Это объясняется сложностью такой общей модели как при создании, так и при практическом использовании.

Поскольку нарушитель в определенном смысле также является системой, то нецелесообразно создание какой-то общей (или обобщенной) модели нарушителя, одновременно учитывающей названные выше стабильные и изменяющиеся факторы.

Использование понятия «набор моделей нарушителей», позволяет менее болезненно и более адекватно решать ряд вопросов, возникающих в практике концептуального проектирования и оценки эффективности ИСБ.

Опыт по категорированию нескольких тысяч объектов, анализу уязвимости и оценки эффективности ИСБ нескольких сотен различных крупных ОПВН, в процессе которых формируется модель нарушителя, показал, что для выполнения практических задач целесообразно иметь три типа моделей нарушителя, условно называемых как технологическая, оперативная и проектная модели.

Технологическая модель нарушителя (ТМН) разрабатывается как набор характеристик потенциальных нарушителей, при которых эти нарушители будут способны реализовать соответствующие угрозы объекту. Это - минимально необходимое количество нарушителей определенного типа и оснащенности, которое понадобится для реализации конкретной угрозы по определенному сценарию, исходя из особенностей функционирования (то есть технологии и оборудования) объекта. Цель создания этой модели – установить, какими минимальными силами, на каких блоках ИСБ могут быть реализованы угрозы и нанесены те или иные потери объекту, государству обществу.

Параметры данной модели диктуются особенностями объекта и технологичных процессов на нем (и поэтому являются достаточно стабильными).

В силу своего содержания ТМН не учитывает политическую и социальную обстановку вокруг объекта, возможные побудительные мотивы проведения несанкционированных действий, деловые и личные качества персонала объекта и подобные факторы.

Формирование ТМН осуществляется на основании анализа сценариев реализации угроз нарушителями.

Данная модель является экспертно-аналитической. Задача аналитической части, как правило, заключается в определении предметов физической защиты и оценке последствий (потенциальных потерь) от реализации угрозы. Задача экспертной части – отбор сценариев реализации угроз, градация характеристик нарушителей и утверждение совокупности сценариев, которые учитывают при создании концепции модернизации ИСБ.

Упрощенная трактовка одного из элементов ТМН может быть представлена следующим образом: «Чтобы реализовать угрозу **А** по сценарию **Б** необходимо участие не менее **Х** нарушителей типа **С** с такими-то характеристиками». При отсутствии официально утвержденной проектной угрозы для объекта ТМН может служить опорной точкой при обосновании состава и характеристик ИСБ.

Оперативная модель нарушителя (ОМН) разрабатывается как предполагаемый набор характеристик потенциальных нарушителей на текущий момент времени.

Параметры данной модели определяются особенностями окружающей среды (в широком смысле слова) – положением в мире, стране, регионе, районе расположения объекта, социальным климатом в коллективе предприятия, социопсихологическими особенностями отдельных групп людей, так или иначе влияющих на функционирование объекта и т.п. – и поэтому являются достаточно динамичными.

ОМН учитывает возможные мотивы проведения несанкционированных действий криминогенного характера и личные качества персонала объекта, оценку сил ведомств, противодействующих терроризму и криминалу, и определяет характеристики потенциальных нарушителей, способных осуществить какие-либо противоправные действия на объекте на текущий момент времени. Фактически это оценка текущей оперативной обстановке в районе расположения объекта. Упрощенно: «Для свершения события **А** сегодня может быть сформирована группа численностью **Y** нарушителей с такими-то характеристиками. ОМН существенно более динамична, чем ТМН. Формирование ОМН – исключительно экспертная задача. С точки зрения практического использования ОМН является «оселком» для оценки текущих возможностей ИСБ.

Проектная модель нарушителя (ПМН) разрабатывается как набор характеристик потенциальных нарушителей, которым должна успешно противостоять ИСБ объекта. ПМН – это максимальное количество нарушителей определенного качества, реализующих конкретную угрозу по определенному сценарию, действия которых, по мнению государства, должны быть успешно пресечены ИСБ объекта. Упрощенно: «ИСБ объекта

должна быть способна пресечь действия нарушителей типа **C** численностью до **Z** человек с такими-то характеристиками, направленные на реализацию угроза **A».**

Основной целью формирования и утверждения ПМН является распределение усилий между государством (силовыми и другими ведомствами) и ИСБ объекта по пресечению несанкционированных действий нарушителей различных типов и оснащенности (то есть в конечном итоге – задание требований к ИСБ). Кроме того, ПМН используется при оценке эффективности ИСБ с целью проверки ее соответствия предъявляемым требованиям.

Поскольку параметры данной модели диктуются не только особенностями объекта и окружающей среды, но и взглядами государства на проблему противодействия противоправным действиям по отношению к ОПВН и его возможностям в этих вопросах, задача определения ПМН должна решаться не на объектовом, а на государственном уровне.

Задача формирования ПМН является исключительно экспертной. При этом экспертами предлагаются варианты ПМН для конкретных объектов, а должностными лицами государственных органов, уполномоченных принимать решения в рассматриваемой области, с позиции оправданного пессимизма производится утверждение моделей.

Как в методическом, так и в практическом плане наиболее проработаны вопросы, связанные с формированием моделей нарушителей для ядерно-опасных объектов. Изложенные подходы применимы (на наш взгляд применяются) для всех ОПВН. С уверенностью можно сказать, что за рубежом ситуация с разработкой моделей нарушителей во многом определяется как инициативами, так и практическими шагами, которые в этом направлении осуществляет МАГАТЭ. При этом под практическими шагами понимается разработка документов по методологии и методикам формирования перечней угроз и моделей нарушителей.

Один из примеров этих документов – внедренное в 2003 году «Руководство по самооценке риска диверсий на ядерных установках». В настоящее время МАГАТЭ активно занимается разработкой документов, определяющих методику обоснования проектных угроз «Design Basis Threat» (DBT) для ядерно-опасных объектов. Одним из основных элементов DBT является модель нарушителя, «реализующего» угрозу.

Совершенно очевидно, что методология, а во многом и методика формирования DBT одинаковы для ядерно-опасных и других крупных ОПВН.

Анализ имеющихся документов показывает, что разработка DBT за рубежом осуществляется в три (достаточно условно выделенных) этапа:

- полный анализ угроз государству, его элементам и, в первую очередь опасным объектам;
- отсев угроз, которое государство считает маловероятными и незначительными;
- определение проектной угрозы для каждого из объектов, которые попали в надлежащие перечни, и утверждение их (проектных угроз) на соответствующем государственном уровне.

На первом этапе в процессе оценки национальных угроз государство в лице компетентных органов определяет (с учетом мнения руководства) спектр возможных террористических акций, которые могут угрожать объекту. Кроме того, в процессе оценки национальных угроз определяются угрозы, которые не могут быть отражены ИСБ на уровне объекта, а потому учитываются другими государственными органами (структурами).

Второй этап может проводиться на основании методологии, изложенной в «Руководстве по самооценке риска диверсий на ядерных установках». Задача этого этапа – экспертный отсев угроз, которые являются маловероятными, и экспертно-аналитический отсев угроз, потери от реализации которых считаются в государстве допустимым риском.

Третий этап выполняется компетентными государственными органами при активном участии экспертов объектов. Именно на этом этапе при участии экспертов силовых ведомств и объектов принимается решение о разделении задач по защите объектов между государством (ведомствами государства) и объектами (ИСБ и системой технологической безопасности).

Формирование проектной модели нарушителя (и проектной угрозы в целом) – важнейший этап концептуального проектирования, в значительной мере определяющий как эффективность обеспечения защиты любых объектов, так и возможность ее оценки.

Разработка и утверждение проектной модели нарушителя и проектной угрозы представляют собой сложную многоплановую задачу государственного уровня по распределению усилий по защите объектов между государством (ведомствами государства) и объектами (ИСБ и системой технологической безопасности).

Использование на практике описанных выше технологической и оперативной моделей нарушителей способствует адекватной оценке эффективности ИСБ объектов, обоснованному принятию проектных моделей нарушителей и проектных угроз для конкретных объектов и в целом способствует рациональному распределению ответственности между заказчиком и работой интегрированной системы безопасности объектов при решении задачи обеспечения их безопасности.

ИНФОРМАЦИОННЫЕ АСПЕКТЫ БОРЬБЫ С ТЕРРОРИЗМОМ

Е.С. Харабуркина (Тульский филиал Московского университета МВД России)

Борьба с терроризмом – обязанность государства как гаранта прав и свобод человека и гражданина. С этой целью в мировом сообществе заключаются соглашения, направленные на создание эффективных средств и

механизмов предупреждения, выявления, пресечения, наказания лиц, виновных в терактах. Возможно ли ограничение прав и свобод человека в данной ситуации? Если государства начнут склоняться к макиавеллизму – «цель оправдывает средства» – то, по сути, правительства еще больше развяжут руки террористам, и это будет означать фактическую победу последних. Только поместив борьбу с терроризмом в рамки верховенства права, можно гарантировать признанный на международном уровне стандарт, ставящий терроризм вне закона.

Бывший Генеральный Прокурор РФ В. Устинов отметил, что мы настолько далеко ушли по пути либерализации законов, что эффективно бороться с терроризмом стало сложно. Поэтому, он считает необходимым в законодательстве о противодействии терроризму закрепить меры, недопустимые в иных условиях и неприемлемые в борьбе с другими преступлениями. В частности, упростить процедуру судопроизводства, предусмотреть «контрзахват» заложников, конфискация имущества у членов семьи лиц совершивших террористические акты [5]. Но что могут дать такие меры в отношении людей, которые сами ищут смерти. Подвергая репрессиям их родных и близких, государство фактически будет плодить новых террористов.

В данный момент гражданин в России оказался в ситуации, когда нет ничего тайного, частного, личного. Для его же личного блага он обязан по первому требованию выворачивать карманы, вытряхивать все из сумки и отчаянно удостоверять собственную личность. Конечно, мы можем утешаться мыслью, что это поможет стражам закона выявить настоящего злоумышленника. Однако, где гарантия того, что это не явится первым шагом к созданию нового «полицейского государства».

Таким образом, в условиях угрозы терроризма мир ступил на зыбкую почву обеспечения безопасности граждан за счет личной свободы каждого из них. То есть права и свободы человека нарушаются якобы ради него самого. Международное сообщество фактически отказалось от господствующей долгое время парадигмы о не допустимости ограничения демократических прав и свобод человека в целях противодействия терроризму, так как данные меры ведут к усилению вмешательства государства в личную жизнь граждан, снижают уровень контроля общества за деятельностью государства [4]. В настоящее время общественная безопасность рассматривается как приоритетный фактор, позволяющий «отодвинуть на второй план» права каждого отдельного члена общества [2, с. 95].

Однако Министр внутренних дел России Р. Нургалиев признал, что «система противодействия терроризму носит не предупредительный и упреждающий характер, а только реагирующий» [5]. Поэтому, ужесточая борьбу с насилием, важно самим не ожесточаться. Да, в борьбе с терроризмом, видимо, без временного ограничения каких-то свобод не обойтись. Но только силовыми средствами искоренить терроризм нельзя. Нужны продуманные, скоординированные, коллективные акции всего мирового сообщества по устранению причин, ведущих к распространению террора:

1. Необходимо договориться о том, что понимать под терроризмом.
2. Любые силовые акции против государств, поддерживающих террористов, должны проводиться только по решению всего мирового сообщества.
3. Выслеживанию террористов, устранению их финансовой подпитки, ужесточение контроля за оборотом оружия необходимо внутри единой информационной системы, в условиях постоянного обмена информацией между спецслужбами.
4. Основные усилия мирового сообщества должны быть направлены на ликвидацию социально-экономических корней терроризма.
5. Настоятельной необходимостью становится система мер по воспитанию подрастающего поколения в духе терпимости, позитивного отношения к людям других культур и конфессий, по налаживанию взаимопонимания между представителями разных религий и цивилизаций.

Выслеживание террористов, устранение их финансовой подпитки, ужесточение контроля за оборотом оружия необходимо проводить внутри единой информационной системы, в условиях постоянного обмена информацией между спецслужбами. Для борьбы с международным терроризмом необходимо объединение усилий всех государственных и общественных структур. В условиях такой борьбы сохранение демократии возможно лишь при всемерном развитии институтов гражданского общества. Только все мировое сообщество способно сообща решить проблему.

В наш информационный век, в век глобализации всех сфер жизнедеятельности общества крайне важным является фактором, способным повлиять практически на все, является информация. Единственная гарантия успешной борьбы с терроризмом – постоянное сотрудничество разведслужб, полиции и правосудия всех стран, одновременно необходимо четко определить пределы, которые государствам не следует переступать при ведении борьбы с терроризмом [1, с. 17]. Меры по борьбе с терроризмом будут носить законченный характер, только если они применяются в едином информационном пространстве.

Современное демократическое общество, столкнувшись с масштабными актами международного терроризма, создающих угрозы основополагающим ценностям и принципам либерального общества, вынуждены использовать меры репрессивного характера, связанные с использованием вооруженной силы и все более ограничивающие права человека. Научное сообщество и политическая элита в обозримой перспективе рассматривают массовое ограничение основополагающих прав и свобод человека как единственно действенную меру борьбы с международным терроризмом. Однако, данный путь является тупиковым, т.к. фактически способствует достижению целей, преследуемых международным терроризмом – уничтожение либерального общества [1, с. 22]. Как справедливо отмечает Р. Мюллерсон, возможность ограничения прав и

свобод личности по соображениям обеспечения интересов общества в целом или прав и свобод других лиц всегда таит в себе угрозу если даже не злоупотреблений, то во всяком случае принятия несоразмерных охраняемому общественному интересу ограничительных мер [3, с. 163].

Таким образом, государство обязано защищать любое лицо от терроризма, но эта борьба не должна порождать произвол, она должна быть основана на принципе верховенства закона. Иными словами, любые антитеррористические действия должны быть законны и обоснованы, в свою очередь любое ограничение прав и свобод человека должно быть необходимым, пропорциональным данной ситуации, и, самое главное, – правомерным. Однако, как и в российском законодательстве, так и в законодательствах других стран наблюдается несоответствие нормам и принципам международного права, в результате чего происходит неправомерное ущемление прав и законных интересов человека в условиях борьбы с терроризмом.

В современных условиях эффективное противодействие международному терроризму требует, с одной стороны, координации усилий международного сообщества по противодействию террористам, в том числе с использованием мер ограничивающих права человека, с другой стороны, повышение уровня международного контроля по обеспечению прав и свобод человека.

Литература

1. *Бушуев И.И. Демократия и терроризм: цена безопасности (возможно ли бороться с терроризмом с помощью террора?) // Сборник научных трудов. Правовые и социальные исследования. Тула, 2007. Выпуск 2.*

2. *Волкова Н.С. Общественная безопасность и законодательство о правах человека // Журнал российского права. 2005. № 2. С.95.*

3. *Общая теория прав человека. / Отв. ред. Е.А. Лукашева. – М., 1996. С.163*

4. *Пчелинцев С.В. Новое законодательство о противодействии терроризму и ограничения прав и свобод граждан // Журнал российского права. 2006. №5.*

5. *Российская газета. 2004. 30 октября.*

СОВРЕМЕННЫЕ МЕТОДЫ И ИНСТРУМЕНТЫ ОЦЕНКИ УЯЗВИМОСТИ, ЭФФЕКТИВНОСТИ ИНЖЕНЕРНО-ТЕХНИЧЕСКОЙ И ФИЗИЧЕСКОЙ ЗАЩИТЫ ОСОБО ВАЖНЫХ ОБЪЕКТОВ

К.т.н. С.М. Ревин, к.т.н. Д.Д. Грачёв (ГК ВВ МВД России)

Одним из наиболее существенных источников опасности по критерию вероятного ущерба являются критически важные объекты промышленности, транспорта, и других отраслей народного хозяйства.

Физическая защита объектов одна из важнейших компонент комплексной безопасности. Основополагающим принципом построения системы физической защиты является ее адекватность существующим и прогнозируемым угрозам. Оценка уязвимости и эффективности системы физической защиты позволяют получить количестенные параметры этого сооответствия.

Проблема оценки эффективности СФЗ вытекает из самой природы предметной области. Охрана объектов предназначена для минимизации, а в пределе для полного исключения ущерба владельцам объектов в результате умышленных действий нарушителя.

Ущерб возникает в результате:

- уничтожения, повреждения или хищения материальных, информационных и культурных ценностей;
- невосполнимых или санитарных потерь персонала объекта и населения в районе его расположения;
- осложнения социально-политической и (или) экологической обстановки в окрестностях объекта в результате происшествий на объекте вызванных акциями нарушителя.

Затраты на создание и содержание СФЗ можно признать экономически целесообразными в том случае, если они не превышают сумм, необходимых для компенсации возможного ущерба от акций нарушителя.

Необходимо так же учитывать вероятность совершения нарушителем акций приводящих к тому или иному объему ущерба. Стоит ли затрачивать немалые средства для предотвращения практически невероятных вариантов акций? В этом контексте возникает еще один аспект проблемы. С повышением эффективности СФЗ вероятность акций нарушителя снижается. Со снижением вероятности совершения акций снижается необходимость и, как следствие мотивированность руководства предприятия к совершенствованию СФЗ. С другой стороны, с повышением эффективности СФЗ нарушитель вынужден применять все более изощренные средства совершения акций.

С точки зрения нарушителя акция целесообразна, если полезный для нарушителя эффект превышает затраты на совершение акции. Немаловажным аспектом целесообразности совершения акции является оценка нарушителем вероятности быть задержанным или пораженным силами и средствами СФЗ в ходе акции. Практика совершения террористических актов последних лет показывает, что в целом ряде случаев террористы пренебрегают такой опасностью и применяют тактику террористов – смертников. Уровень технической оснащенности и характер применяемых диверсионных средств свидетельствует, что существенное повышение затрат на совершение акций далеко не всегда останавливает организаторов акций. Особенно это характерно для акций, рассчитанных на резонансный социально-политический эффект.

Однако налицо явно выраженная закономерность, которая заключается в том, что повышение

эффективности СФЗ вынуждает нарушителя совершенствовать тактику совершения акций, в том числе и путем увеличением затрат. Это, в свою очередь, обуславливает необходимость совершенствования СФЗ, что ведет к увеличению затрат на ее содержание. Этот процесс носит итерационный характер.

Для определения уровня необходимой достаточности СФЗ остро необходим инструмент оценки ее эффективности и прогнозирования основных направлений развития.

При апостериорном подходе анализируется эффект функционирования СФЗ за определенный прошедший период. В качестве показателя эффективности используется отношение количества пресеченных попыток акций нарушителя за рассматриваемый период к общему числу зарегистрированных попыток. При всей простоте и точности подхода возникает два источника неопределенности. Первый состоит в невозможности прямого учета незарегистрированных попыток нарушителя. Косвенная оценка может быть получена, например, по результатам инвентаризации имущества и то, только для акций имеющих целью хищение материальных ценностей.

Еще более сложно учесть количество планировавшихся попыток, но не осуществленных ввиду отказа нарушителя от реализации планов ввиду сложности преодоления, имеющейся на объекте СФЗ.

Неопределенность так же возникает в случае, когда за исследуемый период не зарегистрировано ни одной попытки акции.

Апостериорный подход так же не дает ответа на вопрос об эффективности СФЗ в отношении любой из возможных в будущем других типах акций.

Априорный подход заключается в оценке вероятности пресечения силами и средствами имеющейся на объекте СФЗ возможной в будущем акции нарушителя. Существенным недостатком априорного подхода является практическая невозможность рассмотреть все возможные цели (стратегии) и способы (тактики) акций нарушителя. В этом случае, можно прогнозировать только эффективность СФЗ в отношении четко сформулированного множества моделей акций нарушителя. В отношении остальных акций остается ситуация неопределенности.

Интуитивно-рациональный метод

Метод заключался в использовании здравого смысла и опыта должностных лиц, на которых возлагается ответственность за охрану объектов. История знает не мало весьма эффективных СФЗ созданных таким методом. В них нередко применялись изощренные ловушки для нарушителя, ложные объекты, средств сигнализации и скрытного наблюдении. Системы, созданные таким методом, практически не подлежат объективной типизации, как правило, не документированы и плохо приспособлены к тиражированию примененных организационных и технологических решений.

Однако, и сегодня интуитивно-рациональный метод достаточно широко применяется при проектировании СФЗ, в том числе и специализированными проектными организациями, выполняющими проектирование СФЗ даже для особо важных объектов.

В рамках этого метода ярко выражена процедура генерации вариантов построения и функционирования СФЗ. Процедура анализа и оценки не формализована и выполняется интуитивно и подспудно проектировщиком на основании субъективной системы приоритетов и предпочтений. В современном обществе наблюдается тенденция в создании корпоративной культуры обеспечения комплексной безопасности объектов. Система физической защиты, как одна из важнейших компонент комплексной безопасности неизбежно попадает в разряд централизовано регламентируемых видов деятельности. В этих условиях наиболее ярко проявляются сущностные недостатки интуитивно-рационального метода обусловленные его ярко выраженной субъективностью.

С целью повышения объективности оценки эффективности СФЗ возник метод натурных экспериментов, наиболее распространенным вариантом, которого является метод тактических учений.

Метод натурных экспериментов

Метод привлекает простотой его реализации и наглядности результатов. Метод реализуется поэтапно. На подготовительном этапе определяется перечень объектов, подлежащих исследованию. Формулируются цели эксперимента и совокупность ограничений и допущений. Разрабатывается один или несколько сценариев проведения эксперимента. Осуществляется формирование, оснащение и подготовка группы имитирующей действия нарушителя по каждому из принятых сценариев. При необходимости проводятся тренировки. Разрабатывается методика наблюдения и документирования действий «нарушителя», а так же сил и средств физической защиты.

В основной фазе эксперимента осуществляются действия обозначающей нарушителя группы реализующей заданные сценарии акции. Наблюдаются и документируются процессы реализации «акции нарушителя» и функционирования СФЗ.

В третьей фазе эксперимента осуществляется детальный разбор действий и достигнутых результатов, формулируются выводы и рекомендации по совершенствованию СФЗ.

Чаще всего эксперимент проводиться в форме тактических учений.

Метод, естественно, имеет и ряд существенных недостатков.

1. Сценарии эксперимента должны учитывать требование минимизации осложнений для функционирования объекта по прямому предназначению, так как эксперимент проводится на действующих объектах без остановки основного производства.

2. При проведении эксперимента, как правило, предусматриваются сценарии, ограничивающие разрушающие воздействия на элементы СФЗ и исключающие потери и трамвирование персонала участвующего в эксперименте.

3. Проведение эксперимента требует достаточно серьезных временных, организационных и материальных затрат.

4. У организаторов и участников эксперимента чаще всего существует соблазн или подсознательное стремление создать условия для положительных результатов эксперимента в ущерб объективности.

5. При планировании эксперимента практически невозможно реализовать набор статистически представительных наборов данных путем многократного повторения действий даже при ограниченном количестве сценариев.

6. Жесткая привязанность действий участников эксперимента к сценариям исключает проявление участниками эксперимента инициативы, «военной хитрости», использование взаимного психологического воздействия на персонал противоборствующих сторон.

В настоящее время метод применяется достаточно широко в основном на особо важных объектах с войсковой охраной. Например, подобные учения регулярно проводятся на объектах ядерно-энергетического комплекса. В ходе этих учений для обозначения действий нарушителя привлекаются подразделения специального назначения спецслужб.

Методы экспертной оценки

В классе классических методов оценки эффективности СФЗ методы экспертной оценки представлены достаточно широко. Можно выделить два основных типа таких методов. К первому типу можно отнести методы аудиторской проверки, которые состоят в оценке соответствия состава, структуры, функциональных возможностей и эффективности функционирования СФЗ федеральным, ведомственным или корпоративным стандартам. Эти стандарты, как правило, содержаться в нормативно правовых или организационно распорядительных документах.

Альтернативой аудиту выступают методы статистической обработки мнений группы независимых экспертов. К этой группе можно отнести методы: квалиметрии, анализа иерархий, согласования групповых решений и т.п. В данной работе не ставиться задача подробного описания применения методов экспертной оценки к предметной области анализа эффективности СФЗ, достаточно полно описанных в многочисленных изданиях, посвященных данной тематике.

Полезность полученных прогнозов и оценок сильно зависит от уровня компетенции и опыта привлекаемых экспертов. Не меньшее значение имеет и методика анализа и интерпретации мнений экспертов. Но в любом случае в результате применения данного метода на выходе получается усредненное субъективное мнение специалистов данной предметной области, отражающее устоявшиеся взгляды и заблуждения, научные и политико-психологические особенности личности и т.п. Не стоит исключать и возможность ангажированности или личной заинтересованности экспертов в характере результатов оценки эффективности той или иной СФЗ.

Методы **логико**-вероятностного моделирования.

Получение объективных априорных оценок СФЗ возможно методами математического моделирования. Наибольшее распространение до недавнего времени получили логико-вероятностные модели.

Следует разделить все множество логико-вероятностных моделей на аналитические и имитационные. Аналитические модели построены на основе уравнений и на их выходе можно получить оценку эффективности СФЗ в виде значения вероятности совершения или пресечения акции нарушителя.

Имитационные модели в основе использующие метод статистических испытаний (метод Монте-Карло) оперируют параметрами законов распределения вышеуказанных величин.

1.1 Аналитические модели

Простейшие аналитические логико-вероятностные модели рассматривают акцию нарушителя как некую последовательность событий, каждое из которых наступает с некой вероятностью. В общем случае задача сводиться к построению графа возможных событий в виде дерева, корнем которого является начало акции нарушителя. Дерево, чаще всего, имеет два конечных события: «акция пресечена» и «акция совершена». Полный набор возможных путей на таком графе описывает все множество возможных сценариев развития ситуации. Каждый путь представляет собой цепочку событий.

Присвоив каждому из событий значение вероятности его наступления не сложно вычислить эффективность СФЗ для каждого сценария акции нарушителя. Если последствия каждой акции в модели одинаковы, то за общую эффективность СФЗ следует принять наименьшее из полученных значений вероятности пресечения акции нарушителя. Соответствующая этому значению цепочка событий представляет собой так называемый «критический путь» нарушителя. Это последовательность действий приводящих к успешному совершению акции с наибольшей вероятностью. Требование одинаковости последствий для каждой из ветвей графа выполняется только в случаях, когда цель акции одна и та же. Это означает, что акция выполняется в отношении единственного предмета охраны, расположенного в одном и том же месте, в одном и том же количестве и с ним выполняются одни и те же действия каждый раз одинаковым способом.

Если цели акций различны или различны способы их совершения, то для каждого сочетания

необходимо построить свое дерево событий и повторить вычисления. В этом случае мы получаем для каждого дерева «критический путь» и в результате множество пар «размер последствий акции – вероятность ее совершения».

Можно пренебречь практически невероятными вариантами и акциями с незначительными последствиями. Однако критерии маловероятности и незначительности последствий приходиться устанавливать субъективно или методами экспертных оценок.

Боле подробные и чувствительные варианты логико-вероятностных моделей строятся на основе хорошо известных теорий: аппарат цепей Маркова; теория массового обслуживания; теория игр и т.п. Наряду с известными достоинствами, каждый их подходов имеет и свои недостатки и ограничения.

Аналитические модели достаточно удобны для анализа сравнительно небольших подсистем СФЗ, таких как участок периметра, отдельное охраняемое помещение, небольшое режимное здание.

1.2 Имитационные модели

Имитационное моделирование используется тогда, когда размерность модели становиться достаточно большой и (или) имеются затруднения с точностью исходных данных, когда объемы вычислений для полных групп различных комбинаций исходных данных превышают разумный (или отведенный) режим времени.

При имитационном моделировании необходимо построение тех же графов, что и в аналитической модели. Однако, выбор дерева, выбор каждого шага пути по графу и исход каждого события на пути осуществляется методом розыгрыша. Розыгрыш состоит в вычислении случайного значения разыгрываемой вероятности на основе заданных законов ее распределения. Для получения требуемых (необходимо достаточных) точностей осуществляется соответствующее количество прогонов имитационной модели. Точность имитационного моделирования заведомо ниже аналитического. Точность, так же как от количества розыгрышей, зависит от правильности выбора законов распределения используемых случайных величин и качества используемого датчика случайных чисел нормально распределенных на интервале от 0 до 1.

Практика имитационного моделирования СФЗ показывает, что этот метод применим для относительно небольших объектов. С ростом размерности графа наблюдается лавинообразный рост объема необходимых исходных данных с одновременным снижением чувствительности модели к изменениям частных параметров в узлах графа.

1.3 Метод виртуальнореальностного ситуационного моделирования.

Возрастающие возможности широко доступных компьютеров создают условия для все более совершенных методов анализа эффективности систем физической защиты объектов. Ярким примером этого класса моделей является модель, положенная в основу программного комплекса «Итерация» производства ЗАО «Итерация».

Основная идея метода состоит в гармоничном объединении технологий виртуальной реальности и человеческого интеллекта специалистов предметной области.

Технологиями виртуальной реальности создается трехмерная реалистическая модель объекта и прилегающей территории. В модельном пространстве создаются анимированные управляемые модели людей, обозначающие бойцов сил охраны и нарушителя. Создаются модели вооружения, транспортных средств и боевых машин, модели средств совершения акции и элементов комплекса инженерно-технических средств физической защиты.

Свойства моделей и программные интерфейсы позволяют пользователям создавать произвольный набор ситуаций и отрабатывать на модели различные сценарии акций нарушителя, различные варианты построения и тактики действий системы физической защиты.

Программный комплекс «Итерация» предоставляет разработчикам модели и пользователям полнофункциональный набор программных модулей.

Краткое описание технологии

Технология виртуально-реальностного ситуационного моделирования комплексной безопасности объектов разработана коллективом авторов в 1998 году. Технология непрерывно развивается и совершенствуется. Все права на технологию, методики и специальное программное обеспечение принадлежат ЗАО «ИТЕРАЦИЯ». На ее основе разработаны, внедрены и успешно эксплуатируются аппаратно-программные комплексы «Контрфорс», «Блок-АС», «Итерация-НС», «Итерация – ГРЭС».

Назначение

Информационная технология «Итерация» предназначена для информационно-технологического обеспечения деятельности органов управления и подразделений безопасности стационарных объектов.

На ее основе создается единое информационно-технологическое пространство комплексной безопасности объектов. Это достигается согласованием и утверждением единых форматов сбора, создания и обмена документами, данными, моделями и информационными сообщениями в структурных подразделениях и органах управления всех заинтересованных ведомств в части обеспечения комплексной безопасности объектов с учетом требований режима секретности и разграничения доступа пользователей.

Для обеспечения такой унификации применяется единое специальное программное обеспечение, математические модели и методики, система классификаторов, форматы и протоколы представления и обмена информацией.

Методологическая основа

Методология основана на системном комплексировании возможностей информационных технологий

хорошо зарекомендовавших себя на практике:

1. В качестве общего методологического основания разработки используется системно-конфигурационный подход.
2. Требования к разрабатываемым компонентам формулируются на основе методологии моделирования бинес-процессов служб и подразделений системы комплексной безопасности.
3. Инжиниринг системы осуществляется в итерационном сочетании структурно-функционального и функционально-структурного подходов к синтезу сложных систем.
4. В основу информационной модели и интерфейса отображения результатов моделирования и расчетов положены технологии виртуальной реальности.
5. Системное взаимодействие подключаемых приложений организовано на принципах сервисно-ориентированной архитектуры.
6. В качестве интегрирующего средства используется технология WEB-портала на основе динамического HTML в сочетании с современными архитектурами серверных компонент.
7. Сбор объективных исходных данных для построения трехмерных моделей осуществляется с помощью высокоточного лазерного сканера.
8. Для разработки геотопологических моделей и расчетов на основе пространственно-связанных данных используются методы геоинформационных систем с топологической моделью данных.

Реализованные компоненты

1. Математическая модель и программный комплекс «Итерация» моделирующий функционирование системы физической защиты стационарного объекта.
2. Методика доступа к разнородной пространственно связанной информации (цифровые карты, космоснимки, трехмерные модели) на основе ГИС с топологической моделью данных.
3. Система сбора и обработки данных для создания и редактирования трехмерных моделей на основе высокоточного лазерного цифрового сканирования.
4. Действующий прототип интеграционного WEB- портала.
5. Методика системно-конфигурационного синтеза ситуационных центров в системе комплексной безопасности.
6. Система создания, ведения и актуализации единой базы классификаторов и кодификаторов.

Порядок разработки моделей

Разработка модели СФЗ осуществляется поэтапно. Состав работ:

1. Сбор исходных данных для моделирования с выездом на объект, созданием базы данных чертежей (кадастровых паспортов), цифровой панорамной и пообъектной фотосъемки.
2. Разработка трехмерных моделей зданий, сооружений и коммуникаций объекта. Опционально разрабатываются модели подводной и подземной инфраструктуры и коммуникаций.
3. Разработка трехмерных моделей и первичный ввод свойств элементов комплекса инженерно-технических средств физической защиты (КИТСФЗ).
4. Разработка и текстурирование космоснимком триангуляционной модели рельефа территории объекта и прилегающей местности. Сборка и отладка трехмерной модели объекта для её динамического отображения.
5. Разработка трехмерных моделей, первичный ввод свойств и первичное программирование тактики сил охраны включая, вооружение, элементы оснащения и транспортные средства.
6. Разработка трехмерных моделей, первичный ввод свойств и первичное программирование действий группировок нарушителя, включая элементы оснащения способствующие снижению эффективности КИТСФЗ.
7. Доработка эксплуатационной и пользовательской программной документации. Обучение персонала приемам и методам использования комплекса программ для анализа уязвимости и оценки эффективности системы физической защиты.

Состав исходных данных для разработки модели

1. Генеральный план территории объекта с отметками высот или цифровая модель рельефа.
2. Спутниковый или аэрофотоснимок территории объекта и прилегающей местности.
3. Набор атрибутивных данных или кадастровые паспорта зданий сооружений и коммуникаций.
4. Чертежи фасадов и кровли зданий и сооружений.
5. Поэтажные планы зданий со спецификацией помещений (если требуется разработка моделей функционирования СФЗ внутри зданий).
6. Цифровые панорамные снимки территории объекта и фасадов зданий.
7. План охраны и обороны объекта караулами с пояснительной запиской, раскрывающей тактику действий сил охраны в различных ситуациях.
8. Данные о составе, состоянии и размещении на объекте элементов КИТСФЗ.
9. Данные о численности, структуре групп боевого расчета, вооружении, технике и оснащении личного состава караулов. Данные об уровне подготовки персонала в объеме моделируемых параметров.

Типовые функциональные свойства продукта

Трехмерная модель объекта

Все элементы составляющие модель выполняются в виде отдельных файлов в формате *.3ds, после

чего вносятся в базу данных модели и появляются в пространстве моделирования. Элементы модели тектурируются растровыми изображениями, полученными в ходе натурной цифровой фотосъемки. Геометрические характеристики модели должны соответствовать точности исходных данных (чертежей, результатов цифрового лазерного сканирования или натурных измерений).

Модели элементов объекта размещаются согласно генеральному плану объекта и результатам панорамной фотосъемки на координатно привязанной модели рельефа территории которая текстурируется космо- или аэрофотоснимком. На модели рельефа размещаются внутриобъектовые и прилегающие дорожные сети, местные предметы, растительность и элементы ландшафтного дизайна. Размещение рекламных изображений присутствующих в оригинале или вносимых в модель оговаривается отдельно.

Степень детализации элементов модели оговаривается при разработке технического задания с учетом возможностей применяемых вычислительных систем. Модель должна обеспечивать анализ просматривоемости, простреливаемости пространства проходимости местности по дорогам и вне дорог.

Коммуникационная подсистема модели объекта должно обеспечивать корректное моделирование перемещения персонажей с вооружением и оснащением по рельефу, по дорогам, по сооружениям, лестницам, переходам, коммуникациям и другим элементам модели в различных условиях моделируемой обстановки.

Модель КИТСФЗ

Модель комплекса инженерно-технических средств физической защиты включает модели сенсоров, физических барьеров и эффекторов (средств воздействия на нарушителя), объединенных в элементарные участки физической защиты. В качестве элементарных участков рассматриваются: участок запретной зоны; проход (проезд КПП); режимное помещение и т.п. Элементарные участки объединяются в функциональные группы: запретная зона по периметру объекта; локальная зона; режимное здание; КПП и т.п.

Программное обеспечение предоставляет интерфейс создания моделей устройств ИТСО и сборки из них элементарных участков, ввода и редактирования их свойств и сохранения созданных моделей в базе данных.

В модели реалистично отображаться внешний вид устройств, включая основные конструктивные особенности.

В модели предусматривается оснащение персонажей средствами ухищренного преодоления элементов комплекса ИТСФЗ. Для каждого элемента комплекса имеется возможность ввода корректирующих коэффициентов свойств при использовании нарушителем средств ухищренного преодоления.

Интерфейс пользователя предоставляет возможность размещения в модели объекта как интегрированных элементарных участков СФЗ, так и отдельных элементов комплекса.

Модель нарушителя

Модель нарушителя включает модели людей, модели индивидуальной и групповой тактики действий при совершении акций.

Люди представляют собой анимированные скелетно-мышечные модели, оснащенные вооружением, снаряжением, средствами преодоления элементов КИТСФЗ, и средствами совершения акций. Имеется возможность вводить для каждого персонажа психолого-мотивационные характеристики, выражающиеся в стиле его поведения при встрече с противником, а так же в ходе огневого и силового противодействия.

Программное обеспечение представляет возможность визуального программирования тактики действий персонажей и их групп. В модели имеется возможность создания нескольких групп нарушителя произвольного состава и оснащения, назначить группам и отдельным бойцам различные цели и способы совершения акций. Имеется возможность задания маршрутов перемещения бойцов нарушителя тремя способами:

- указанием точного подробного маршрута движения
- указанием начальной и конечной точки маршрута. Нарушитель сам выбирает оптимальный путь в модели объекта.
- указанием начальной и конечной точки маршрута, а так же промежуточных точек обязательных к посещению при выдвижении в конечную точку. Путь между фиксированными точками выбирается нарушителем произвольно.

Модель сил охраны.

Модель сил охраны включает модели людей, индивидуальную и групповую тактику действий. Модели людей и индивидуальная тактика действий сил охраны и нарушителя идентичны.

Групповая тактика точно соответствует плану охраны и обороны объекта, действующим инструкциям и регламентирующим документам. В модели сил охраны, как правило, предусматривается:

- часовые основных и дополнительных стационарных постов;
- основные и дополнительные патрули и подвижные посты;
- тревожная группа;
- группа блокирования
- резерв.

Бойцы сил охраны могут оснащаться средствами индивидуальной бронезащиты различного класса, средствами связи и наблюдения. В модели предусмотрен маневр силами и средствами при изменениях обстановки.

В группировку сил охраны включаются транспортные и боевые машины. Моделируется посадка персонажей в машины в соответствии с назначенной в модели вместимостью, перемещение по дорогам и вне дорог в соответствии с графом проходимости местности, высадка из машин, наблюдение и ведение огня из стрелкового оружия в ходе движения.

Для боевых машин моделируется защита бронированием, наличие вооружения и его свойства.

Интерфейс пользователя.

Пользователю предоставляется интуитивно понятный интерфейс, обеспечивающий интерактивный режим работы. Программный комплекс интерфейсно разделен на модули:

- модуль управления розыгрышем;
- редактор модели объекта;
- редактор плана охраны и обороны;
- редактор персонажей;
- редактор типовых устройств.

Все модули работают с объектами единой модели и с единой базой данных. Ввод, редактирование и удаление элементов и акторов модели и их характеристик и свойств осуществляется в единообразно построенных диалоговых окнах и при помощи системы экранных меню.

Стиль оформления элементов управления (тема) может быть изменена пользователем в соответствии с личной системой предпочтений.

Алгоритм применения СПО «ИТЕРАЦИЯ» для совершенствования СФЗ объекта

- Изучить руководящие документы по организации физической защиты объектов ведомства.
- Собрать необходимые исходные данные для моделирования СФЗ
- Создать и утвердить у заказчика модель нарушителя.
- Создать трехмерную модель объекта физической защиты.
- Разработать план исследований уязвимости (план вычислительного эксперитмента).
- Провести необходимое количество сеансов моделирования.
- Провести статистическую обработку результатов моделирования.
- Подготовить отчет и презентацию результатов администрации.
- Провести «мозговой штурм» по совершенствованию СФЗ и выработать гипотезы.
- Повторить пункты 4,5,6,7 для каждой гипотезы и сравнить полученные результаты для выбора оптимального.
- При необходимости итерационно повторить пункты 8 и 9 требуемое количество раз.

Дополнительные функциональные возможности

Технология СПО «ИТЕРАЦИЯ» позволяет использовать создаваемые модели и программные модули для целей не связанных непосредственно с обеспечением безопасности.

1. Режим информационно-справочной системы.

Создаваемая в процессе моделирования геометрически точная, координатно-привязанная трехмерная модель объекта документирует точное состояние объекта на момент моделирования. С помощью редактора модели объекта можно оперативно вносить изменения в модель параллельно с изменениями в структуре объекта и прилегающей местности. Сохранение версий базы данных при каждой модификации обеспечивает создание трехмерной истории конфигурации объекта.

Каждое здание, сооружение, коммуникация, элементарный участок КИТСФЗ связан с базами данных атрибутивной и присоединенной информации.

В разделе атрибутивной информации вносятся данные о наименовании, номере здания, его предназначении, категории в различных системах категорирования, владельце, балансодержателе, контактная информация дежурных и ответственных лиц. Пользователю с правами администратора предоставляется возможность вносить дополнительные разделы атрибутивной информации. Например, численность персонала по сменам, перечни основного оборудования и.т.п. Наиболее значимая для пользователя информация вносится в справочную ссылку, отображаемую на экране при наведении на здание курсора «мыши». Окно с полной атрибутивной информацией в этом случае выводится при щелчке по правой кнопке манипулятора.

Присоединенная информация представляет собой ссылки на внешние файлы и данные, содержащиеся во внешних информационных системах доступных пользователю в соответствии со схемой регламентирования доступа к информации. Это могут быть чертежи, схемы, трехмерные модели, пояснительные записки, графики работы персонала, базы данных установленного оборудования, расчеты затрат на обслуживание инфраструктуры, кадастровые паспорта и другие информационные ресурсы.

Отдельными разделами могут формироваться базы данных специализированных информационно-справочных систем, таких как кабельное хозяйство, водопровод и канализация, электроснабжение и т.п. Отдельным разделом оформляется информационно-справочная система по комплексу инженерно-технических средств физической защиты.

2. Режим информационно-технологической поддержки деятельности должностных лиц функциональных подразделений.

Для информационно-технологической поддержки должностных лиц СПО «ИТЕРАЦИЯ» включает:

Набор ссылок на документы нормативно-правовой базы:

Базу данных организационно распорядительных документов (положения о структурных подразделениях, регламенты, графики выполнения работ, графики отпусков, функциональные обязанности должностных лиц, табели постов, различного рода планы и т.п.). Документы содержаться в базах данных системы или доступны в виде файлов через систему ссылок.

Для облегчения разработки организационно распорядительных документов и обеспечения строгого соблюдения корпоративного стандарта на форму, содержание и стилевое оформление документов предусмотрен механизм создания и использования набора типовых шаблонов и образцов документов. Для разработки схем и рисунков в системе предусмотрен механизм создания и использования библиотек условных знаков, содержащих 2D и 3D варианты отображения.

3. Режим для ведомственного (корпоративного) ситуационного центра.

СПО «ИТЕРАЦИЯ» в режиме адаптированном для ситуационного центра обеспечивает работу в едином интерфейсе со всеми моделями объектов ведомства (организации, корпорации).

Все модели объектов с дополнительными функциональными модулями хранятся на сервере ситуационного центра. Пользователям предоставляется интерфейс выбора модели и доступа к дополнительным информационным ресурсам моделируемого объекта.

На ситуационном центре СПО «ИТЕРАЦИЯ» используется в качестве информационной справочной системы и для проведения вычислительных экспериментов для ответов на вопросы «что будет, если….?» в процессах информационно аналитической работы, мозговых штурмов, обоснования решений и сравнительного анализа их вариантов.

Результата вычислительных экспериментов на моделях, вместе с результатами обработки статистических данных и отчетными документами хранятся в едином формате. Доступ к аналитическим материалам осуществляет администратор, в соответствии с утвержденной матрицей прав доступа к информации.

ИСПОЛЬЗОВАНИЕ МЕТОДОВ МОДЕЛИРОВАНИЯ ДЛЯ ИССЛЕДОВАНИЯ СИСТЕМЫ ФИЗИЧЕСКОЙ ЗАЩИТЫ ВАЖНЫХ ГОСУДАРСТВЕННЫХ ОБЪЕКТОВ

К.т.н., профессор В.И. Кирин (Академия управления МВД России), А.С. Олейник (ГК ВВ МВД России)

Натурные испытания разрабатываемых систем физической защиты затруднительны, поэтому основной методикой их исследования становится моделирование с учётом конкретных особенностей.

Главное преимущество моделей состоит в том, что они являются удобным инструментом для изучения особенностей функционирования системы физической защиты важных государственных объектов (СФЗ ВГО). Модели позволяют оценить варианты деятельности подразделений внутренних войск по охране таких объектов в тех или иных условиях, проанализировать возможные сценарии действий, предложить и сразу опробовать различные способы совершенствования защиты.

В ситуации, когда натурный эксперимент невозможен, модели являются удобным и доступным инструментом исследования путей совершентвования системы физической защиты важных государственных объектов.

В нашем случае налицо две противоборствующих стороны (нарушители и силы охраны важного государственного объекта), преследующие противоположные цели, причём результат проведения каждого мероприятия одной из сторон зависит от того, какой образ действия выберет противник. Такие ситуации относятся к конфликтным. Любая ситуация, возникающая в ходе военных действий, принадлежит к конфликтным ситуациям.

Исследование военных действий проводилось многими учёными с помощью математических моделей и методов для принятия и поддержки управленческих решений.

Еще в 1915 году двое ученых, англичанин Ф. Ланчестер и русский М. Осипов, независимо друг от друга создали основы математической теории и вывели уравнения взаимного поражения участвующих в нём противников. Результаты их исследования легли в основу современной математической теории боя.

Так в некоторый фиксированный момент времени изменение средней численности сторон за малый промежуток времени τ в зависимости от скорострельности описывается следующим образом:

$$\Delta n_1 = -Л_2\, n_2 \tau,$$

Деля оба уравнения на τ и при $\tau \longrightarrow 0$, имеем систему линейных дифференциальных уравнений, описывающих изменение численности противоборствующих сторон:

$$\begin{cases} \frac{dn_1}{dt} = -Л_2\, n_2, \\ \frac{dn_2}{dt} = -Л_1\, n_1. \end{cases} \qquad (1)$$

Уравнения (1) являются уравнениями динамики боя или уравнениями Ланчестера 2-го рода.

Во второй половине прошлого века, в конце 60-х годов, благодаря использованию ЭВМ и дальнейшего

развития теории и методов моделирования процессов вооружённой борьбы стала возможна реализация идеи создания моделей крупномасштабных операций войск. Нужна была новая прикладная теория моделирования для процессов, отличающихся высокой степенью неопределённости и сложности. Так В.Н. Цыгичко исследовал модели в системе принятия военно-стратегических решений в СССР и предложил свою математическую модель стратегической операции на континентальном театре военных действий.

Такие учёные, как А.Н. Катулев и Н.А. Северцев, исследовали математические методы в системах поддержки принятия решений.

С.В. Баленко исследовал модели и методы управления операциями специального назначения.

А.Ф. Кучков, Н.Ф. Лукашевич, Г.П. Попов, В.В. Шумов осуществляли математическое моделирование служебно-боевых действий пограничных войск.

Проблемы совершенствования управления системой физической защиты важных государственных объектов были предметом исследования таких авторов как С.М. Рёвин, Д.Д. Грачёв и ряда других учёных. Они рассматривали различные аспекты такого совершенствования.

Однако анализ накопленного опыта моделирования показал, что непосредственно для исследования системы физической защиты использование разработанных ранее математических методов и моделей затруднительно. Требуется разработка иного подхода.

В настоящее время для количественного оценивания уязвимости ВГО и эффективности их СФЗ широко используется математическое моделирование. Если по отношению к существующим СФЗ на практике также применяется административно-сверочный и функциональный методы, то для проектируемых систем математическое моделирование является единственным приемом их исследования.

Моделирование, являясь одним из важных путей познания, заключается в воспроизведении свойств исследуемого объекта, процесса или явления с помощью его модели - другого объекта, процесса, явления или абстрактного описания. В математическом моделировании явления внешнего мира сводятся к математическим задачам, для решения которых в настоящее время применяются ЭВМ. Для описания исследуемых объектов используются изображения, уравнения, алгоритмы и программы.

Изучение функционирования СФЗ с помощью ее модели является особым видом эксперимента, в котором модель одновременно является и объектом исследования, замещающим изучаемый объект, и средством исследования. Благодаря этому модельный эксперимент позволяет воспроизводить и изучать функционирование СФЗ в экстремальной его фазе, т.е. при отражении нападения любого нарушителя и при любом сценарии развития событий. В этом состоит главное достоинство моделирования, позволяющего исследовать ситуации, для которых проведение натурного эксперимента затруднено, экономически невыгодно, вообще невозможно в силу его опасности или по другим причинам.

Создание математической модели является важным этапом исследования или проектирования СФЗ. В соответствии с множественностью описания для одной и той же системы можно разработать множество моделей. Они могут иметь разное назначение и отражать те или иные свойства системы, отличаться способом их учета и степенью детализации. Поэтому вид и содержание модели определяются целью исследования.

Так на этапе проектирования СФЗ может оказаться полезным пространственное моделирование зон действия технических средств обнаружения, телевизионного наблюдения и освещения территории объекта. При проведении анализа уязвимости объектов со сложными технологическими процессами в некоторых случаях используется структурно-логическое моделирование для определения наиболее уязвимых мест ВГО (которые могут рассматриваться в качестве целей воздействия диверсантов и террористов) и изъянов в технологических процедурах объекта (прием и отгрузка предметов хранения, выполнение определенных технологических операций и т.п.).

Наиболее же часто, как на этапе проектирования, так и при эксплуатации СФЗ используется модель ее функционирования.

Кроме того, модели функционирования применяются в обучающих программах и тренажерах, использующихся для подготовки сил охраны.

Моделирование функционирования СФЗ ВГО предполагает воспроизведение в модели действий системы при реализации ею главной своей функции - недопущения неприемлемых действий нарушителей на объекте. Именно с ее выполнением связан основной показатель эффективности СФЗ, значение которого должно быть определено в ходе моделирования, - вероятность своевременного пресечения действий нарушителей $P_{пр}$. Под своевременным пресечением понимается остановка действий нарушителей до выполнения ими поставленной задачи.

Зачастую наравне с показателем эффективности СФЗ используется показатель, количественно характеризующий степень уязвимости объекта, - вероятность успешности действий нарушителей P_y.

Во всех известных моделях функционирования СФЗ тем или иным способом отображаются действия нарушителей, направленные на решение поставленной задачи и ответные действия сил СФЗ.

Аналитическая модель представляет собой набор математических выражений для вычисления искомых характеристик СФЗ как функций от входных параметров модели. Основу модели составляют целевая функция и система ограничений на переменные. Целевая функция выражает характеристику системы, которую требуется вычислить. Это может быть вероятность своевременного пресечения действий нарушителей $P_{пр}$ или вероятность успешности их действий P_y. Входные параметры отображают пространственные, структурные и

технические характеристики системы и ее элементов, ограничения - их допустимые предельные значения.

При имитационном моделировании модель исследуемого объекта воспроизводит алгоритм его функционирования и представляется в виде компьютерной программы. Многократное повторение в модели последовательности связанных детерминированных и случайных событий, отображающих противостояние системы физической защиты нарушителям, сбор и обработка получаемых при этом статистических данных позволяют вычислять характеристики СФЗ. Например, оценка вероятности своевременного пресечения действий нарушителей на некотором маршруте при достаточном числе реализаций в модели процесса преодоления нарушителем системы физической защиты может быть получена как отношение числа реализаций, в которых достигнуто своевременное пресечение, к общему количеству реализаций. Точно так же статистическая оценка $P_{пр}$ могла бы быть вычислена в том случае, если бы имелась возможность проведения натурного эксперимента с большим числом равноценных наблюдений попыток нападения нарушителей на объект при одних и тех же условиях. Очевидно, что это невозможно и на практике натурный эксперимент с определенными ограничениями может быть использован как точечная оценка эффективности СФЗ, в том числе для проверки достоверности результатов имитационного моделирования.

Применение имитационного моделирования позволяет снять рассмотренные выше ограничения в выборе математических средств описания функционирования СФЗ, свойственные аналитическим моделям.

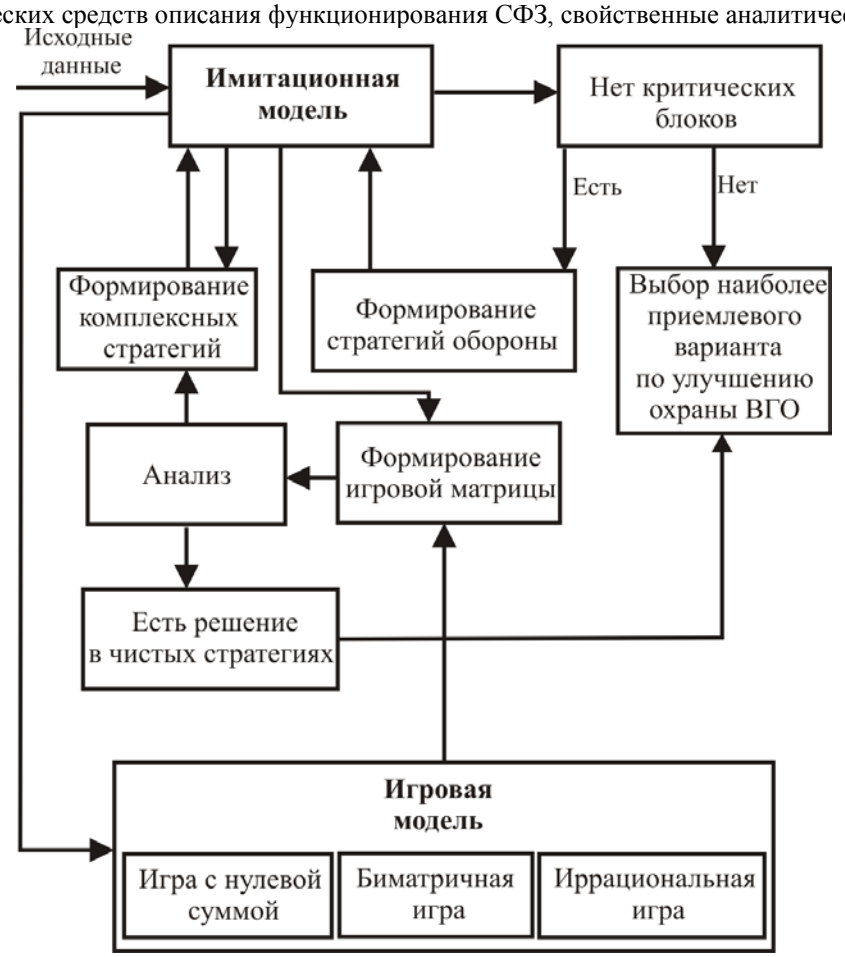

Рис. 2 Структурная схема проведения расчётов по анализу системы физической защиты с использованием имитационной и игровых моделей.

На наш взгляд перспективным направлением является создание комплексной модели на основе применения аналитического и имитационного подходов, что дает возможность использовать достоинства каждого из них. Аналитический подход может быть основан на использовании теории игр. При этом следует учитывать, что в результате имитационного моделирования получаются не сами характеристики СФЗ, а их статистические оценки. Чтобы обеспечить получение точных и надежных оценок (гарантировать принадлежность искомой характеристики некоторому интервалу значений с заданной вероятностью), необходимо проведение достаточного количества испытаний.

На рис. 2 представлена структурная схема проведения расчётов по анализу СФЗ с использованием имитационной и игровой моделей.

На основе компьютерного моделирования могут быть получены необходимые количественные характеристики СФЗ. Их точность в значительной степени определяется полнотой учета основных факторов, оказывающих влияние на эффективность системы, а также точностью исходных данных. Поэтому как на этапе разработки модели СФЗ, так и на этапе ввода в нее исходных данных при проведении анализа уязвимости объекта необходимо участие квалифицированных специалистов. Кроме того, следует отметить большую

трудоемкость, относительно высокую стоимость и значительные временные затраты на моделирование, обусловленные необходимостью сбора и ввода исходных данных, характеризующих конкретный объект. Значительных временных затрат требуют также обработка и интерпретация результатов моделирования.

Данный подход может быть использован для информационно-аналитической поддержки решений в системе управления подразделениями, частями и соединениями по охране важных государственных объектов.