Приложение
к постановлению МПА СНГ
от 16.04.2015 г. № 42-7

Межпарламентская Ассамблея государств – участников Содружества Независимых Государств

РЕКОМЕНДАЦИИ
по совершенствованию законодательства государств – участников СНГ в сфере противодействия технологическому терроризму

1. Общие положения

Рекомендации по совершенствованию законодательства государств – участников СНГ в сфере противодействия технологическому терроризму направлены на установление общих подходов государств – участников Содружества Независимых Государств к правовому регулированию противодействия технологическому терроризму, укреплению и обеспечению сбалансированности национальных правовых систем, обеспечению технологической защищенности, а также на создание условий для безопасного использования потенциально опасных технологий.

Для совершенствования законодательства в сфере противодействия технологическому терроризму требуется надлежащая методологическая база, которая должна обеспечивать адекватное научное представление сущности процессов и явлений в сфере противодействия технологическому терроризму с целью выработки обоснованных мер по улучшению ситуации в государствах – участниках СНГ. Только на такой основе возможна разработка унифицированного пакета правовых документов в сфере противодействия технологическому терроризму. Решение данной задачи требует привлечения имеющегося научного потенциала государств – участников СНГ. В качестве первого шага в решении данной задачи следует рассмотреть методологический подход к гармонизации системы правового регулирования в сфере противодействия технологическому терроризму на пространстве СНГ.

В основу данного подхода положены формируемые на базе актуальных научных знаний представления о современных технологических процессах, о государстве как сложной системе, о сущности явлений и процессов, происходящих в ней, а также о правовом регулировании совместных международных усилий по противодействию технологическому терроризму.

Для реализации ключевых положений таких представлений или общих методологических основ гармонизации системы правового регулирования в рассматриваемой сфере деятельности необходимо:

– учитывать факторы, определяющие специфику технологического терроризма как нового этапа в развитии террористической угрозы;

– организовать взаимодействие специалистов, ведущих научных организаций государств – участников СНГ для выработки общего согласованного методологического подхода к обеспечению безопасности государств – участников СНГ в сфере противодействия технологическому терроризму;

– разработать концепцию обеспечения безопасности государств – участников СНГ в сфере оборота потенциально опасных технологий;

– разработать унифицированный пакет правовых документов по обеспечению безопасности государств – участников СНГ в сфере потенциально опасных технологий.

Основными методами и формами правового и организационного сотрудничества государств – участников СНГ в области противодействия технологическому терроризму являются:

– согласование процедур работы по сближению и совершенствованию законодательства государств в области противодействия технологическому терроризму;

– установление единых правил учета и систематизации угроз технологического терроризма, форм их возможной реализации, фактов нарушения антитеррористического законодательства;

– учет рисков криминального использования потенциально опасных технологий, а также учет выявляемых угроз и фактов правонарушений, снижающих уровень безопасности функционирования потенциально опасных технологий;

– формирование единой системы мониторинга, идентификации и предупреждения террористических атак на объекты оборота потенциально опасных технологий государств – участников СНГ;

– создание единой системы своевременного оповещения и оперативного информирования граждан о чрезвычайных ситуациях, угрозах террористических актов;

– обобщение зарубежного опыта в области противодействия технологическому терроризму;

– обеспечение научного и производственного сотрудничества в области моделирования террористических атак на объекты оборота потенциально опасных технологий и выработка алгоритма ответных действий;

– предотвращение незаконного оборота компонентов потенциально опасных технологий;

– совершенствование оперативно-разыскной деятельности компетентных органов государств – участников СНГ по противодействию технологическому терроризму;

– создание единой системы критериев и методов обеспечения технологической безопасности на базе действующих и разрабатываемых двусторонних и многосторонних конвенций и соглашений;

– организация совместной профилактической работы с персоналом объектов оборота потенциально опасных технологий, расположенных на территории государств – участников СНГ.

Предлагаемый в настоящих Рекомендациях подход к решению проблем правового регулирования в области противодействия технологическому терро-

ризму может способствовать развитию сотрудничества государств – участников СНГ по противодействию другим вызовам и угрозам.

2. Цель, задачи и принципы совершенствования законодательства государств – участников СНГ в сфере противодействия технологическому терроризму

Совместная деятельность государств – участников СНГ в сфере противодействия технологическому терроризму преследует своей целью создание правовых условий для системной реализации и обеспечения защиты сбалансированных интересов личности, общества и государства в рамках противодействия технологическому терроризму.

Задачами правового регулирования отношений в сфере обеспечения противодействия технологическому терроризму являются:

– обеспечение терминологической ясности и согласование понятийного аппарата, используемого при правовой регламентации в сфере противодействия технологическому терроризму;

– развитие эффективных правовых режимов противодействия технологическому терроризму в государствах – участниках СНГ;

– приведение нормативных правовых актов государств – участников СНГ в соответствие с положениями международных договоров и соглашений в данной сфере;

– совершенствование взаимодействия государств – участников СНГ по реагированию на вызовы и угрозы технологического терроризма;

– поиск возможных форм согласования действий по совершенствованию законодательства государств – участников СНГ с аналогичной работой и опытом государств – членов ОДКБ, ШОС и других организаций;

– создание условий для равноправного участия государств – участников СНГ в межгосударственных отношениях по противодействию технологическому терроризму;

– минимизация возможных неблагоприятных последствий, связанных с использованием потенциально опасных технологий в террористических целях;

– использование единого подхода к установлению меры ответственности, соответствующей тяжести преступлений, связанных с использованием потенциально опасных технологий в террористических и иных преступных целях или создающих условия для совершения подобных действий.

Принципами развития законодательства государств – участников СНГ в сфере противодействия технологическому терроризму являются:

– сбалансированность прав, свобод и обязанностей личности, общества и государства в сфере противодействия технологическому терроризму;

– системность и комплексное использование правовых, социально-экономических, политических, информационно-пропагандистских и иных мер противодействия технологическому терроризму;

– эффективное разграничение компетенции субъектов противодействия технологическому терроризму;

– преодоление фрагментарности в правовом регулировании противодействия технологическому терроризму;

– адекватность мер противодействия технологическому терроризму характеру и степени террористической угрозы.

3. Приоритетные направления совершенствования национального законодательства государств – участников СНГ в сфере противодействия технологическому терроризму

Анализ действующего законодательства государств – участников СНГ, модельного законодательства СНГ, а также международных документов и соглашений в области противодействия технологическому терроризму позволяет сделать вывод о целесообразности совершенствования законодательства государств – участников СНГ по следующим направлениям:

– проработка и определение понятийного аппарата, используемого в области правового регулирования в сфере противодействия технологическому терроризму;

– определение рисков, источников угроз и самих потенциальных угроз в рассматриваемой области, их видов, раскрытие их характера;

– определение деяний, признаваемых правонарушениями в рассматриваемой области;

– выявление и последующее устранение причин и условий, способствующих использованию потенциально опасных технологий в террористических и иных противоправных целях;

– предупреждение и пресечение деяний, направленных на нанесение ущерба критически важным объектам;

– выявление и пресечение иной террористической и противоправной деятельности, осуществляемой с использованием потенциально опасных технологий либо направленной на них;

– обеспечение национальной безопасности в сфере потенциально опасных технологий;

– обеспечение прав юридических и физических лиц в условиях использования потенциально опасных технологий;

– обеспечение защиты, в том числе физической, лиц, обладающих специальными познаниями в сфере потенциально опасных технологий;

– создание правовых условий для эффективного оборота потенциально опасных технологий;

– формирование и осуществление единой государственной научно-технической политики в сфере потенциально опасных технологий;

– поддержка государственными ресурсами программ обеспечения безопасности оборота потенциально опасных технологий;

– совершенствование обеспечения межгосударственного сотрудничества в сфере противодействия технологическому терроризму;

– защита государственных секретов и противодействие иностранным техническим разведкам.

Также требуют разработки и закрепления в специальных нормативных правовых актах наиболее важные направления деятельности компетентных государственных органов в сфере противодействия технологическому терроризму:

– определение характера и пределов реализации мер, направленных на пресечение указанных правонарушений, в том числе преступлений;

– мониторинг состояния критически важных объектов на предмет выявления признаков правонарушений, в том числе преступлений, связанных с использованием потенциально опасных технологий в террористических и иных противоправных целях;

– определение объема полномочий и распределение ответственности между компетентными государственными органами.

3.1. Согласование терминологии и понятийного аппарата, используемых при правовой регламентации в сфере противодействия технологическому терроризму

Для согласованных действий и конструктивного межгосударственного взаимодействия требуется однозначность понятийного аппарата. С учетом этого предлагается использовать следующие основные термины и понятия:

антитеррористическая защищенность критически важного объекта – состояние защищенности критически важного объекта, препятствующее совершению на нем террористического акта;

государственный регулирующий орган в сфере оборота потенциально опасных технологий – орган или организация (или система органов и организаций), наделенные правительством государства юридическими полномочиями по осуществлению контроля над потенциально опасными технологиями, включая выдачу официальных разрешений (лицензий), а также по регулированию обеспечения технологической безопасности при их обороте;

защита критически важного объекта – система мер обеспечения безопасности критически важных объектов, реализуемая работниками соответствующего объекта, его службой безопасности во взаимодействии с сотрудниками государственных органов и иных организаций, иными лицами и направленная на выявление и ликвидацию угроз безопасному функционированию объекта, поддержание функционирования объекта постоянно или в определенный промежуток времени, в случае реализации таких угроз – на полное или частичное возмещение вреда, причиненного интересам государства и общества, интересам объекта или эксплуатирующей организации в результате нарушения или прекращения его функционирования;

категорирование потенциально опасных технологий – распределение потенциально опасных технологий на группы (категории) по уровню потенциальной опасности для человека и окружающей среды, осуществляемое в соответствии с рекомендациями компетентных международных организаций и основополагающих международных документов;

контроль над потенциально опасными технологиями – совокупность организационных, правовых, технических и технологических мероприятий, направленных на проверку и обеспечение соответствия фактического состояния потен-

циально опасных технологий требованиям, установленным нормативными правовыми актами;

критически важный объект – объект, нарушение или прекращение функционирования которого окажет значительное негативное влияние на жизненно важные интересы государства и общества в экономической, политической, военной, экологической, гуманитарной и других областях;

мера обеспечения безопасности критически важного объекта – совокупность установленных законодательством и выработанных практикой взаимосвязанных действий, осуществляемых работниками критически важного объекта, в том числе его службы безопасности, во взаимодействии с сотрудниками уполномоченных государственных органов, иных организаций и другими лицами, направленных на охрану и защиту критически важного объекта, а также обеспечивающих соблюдение интересов государства и общества;

незаконный оборот компонентов потенциально опасных технологий – незаконные производство, переработка, использование, хранение, транспортирование, сбыт, приобретение и иные действия, совершаемые с компонентами потенциально опасных технологий с нарушением действующего законодательства;

потенциально опасные технологии – технологии, использование которых создает реальную угрозу возникновения чрезвычайной ситуации техногенного характера;

противодействие незаконному обороту компонентов потенциально опасных технологий – система организационных, правовых, научно-технических и оперативно-разыскных мероприятий, направленных на предупреждение, выявление и пресечение незаконного оборота компонентов потенциально опасных технологий;

технологическая безопасность – обеспечение устойчивости потенциально опасных технологий при осложнениях, возникающих в связи с неблагоприятными тенденциями или конкретными событиями в государстве;

технологический терроризм – криминальное использование (или его угроза) потенциально опасных технологий с целью воздействия на принятие решения органами государственной власти, органами местного самоуправления или международными организациями, связанное с устрашением населения и (или) иными формами противоправных насильственных действий;

технология – информация о методах и формах, способах и приемах организации деятельности, а также сама деятельность в определенной отрасли;

физическая защита критически важного объекта – совокупность организационных мероприятий, инженерно-технических средств и действий работников подразделения охраны критически важного объекта, направленных на предотвращение несанкционированного проникновения на объект; своевременное обнаружение несанкционированных действий на территории, в помещениях объекта или на прилегающей территории; пресечение несанкционированных действий; задержание пытающегося проникнуть или проникшего на объект нарушителя безопасности критически важного объекта или замедление его проникновения; задержание лиц, подготавливающих, совершающих или совершивших правонару-

шение или преступление на территории, в помещениях объекта или на прилегающей территории.

3.2. Согласование основных направлений противодействия технологическому терроризму в государствах – участниках СНГ

К числу основных направлений противодействия технологическому терроризму в государствах – участниках СНГ следует отнести:

– выявление и устранение причин и условий, способствующих возникновению и распространению технологического терроризма;

– выявление, предупреждение и пресечение действий лиц и организаций, направленных на подготовку и совершение актов технологического терроризма и иных преступлений в сфере оборота потенциально опасных технологий;

– поддержание в состоянии постоянной готовности к эффективному использованию сил и средств, предназначенных для выявления, предупреждения, пресечения технологического терроризма, минимизации и (или) ликвидации последствий его проявлений;

– обеспечение безопасности граждан и антитеррористической защищенности критически важных объектов;

– осуществление мер правового, организационного, оперативного, административного, режимного, военного и технического характера, направленных на обеспечение антитеррористической защищенности критически важных объектов;

– повышение эффективности информационной защиты критически важных объектов;

– прогнозирование, выявление и устранение угроз технологического терроризма, информирование о них органов государственной власти, органов местного самоуправления и общественности;

– разработку и введение в действие типовых требований по обеспечению защищенности от террористических угроз критически важных объектов.

3.3. Согласование правового регулирования в сфере распределения компетенции между субъектами противодействия технологическому терроризму

Для использования в законодательстве государств –участников СНГ предлагаются следующие общие положения, связанные с распределением компетенции органов государственной власти в сфере противодействия технологическому терроризму.

Глава государства осуществляет общее руководство деятельностью по противодействию технологическому терроризму и реализует полномочия:

– по формированию государственной политики в сфере противодействия технологическому терроризму, обеспечения безопасности критически важных объектов, предупреждения и пресечения правонарушений в сфере оборота потенциально опасных технологий и контроля над ними;

– по созданию системы органов государственной власти и определению их компетенции в области обеспечения технологической безопасности критически важных объектов, а также порядка их взаимодействия;

– по определению порядка создания и принципов построения государственной системы реагирования на акты технологического терроризма;

– по утверждению государственных программ в области обеспечения защиты от актов технологического терроризма и в области обеспечения безопасности критически важных объектов;

– по нормативно-правовому регулированию деятельности органов государственной власти в сфере противодействия технологическому терроризму, контроля над технологиями на критически важных объектах.

Правительство государства обеспечивает создание необходимых правовых, экономических, организационных и других условий для противодействия технологическому терроризму и реализует полномочия:

– по обеспечению реализации государственной политики в сфере противодействия технологическому терроризму, обеспечения безопасности критически важных объектов, предупреждения и пресечения правонарушений в сфере оборота потенциально опасных технологий и контроля над ними;

– по организации разработки, утверждения и обеспечения выполнения государственных программ в области обеспечения защиты от актов технологического терроризма и в области обеспечения безопасности критически важных объектов;

– по организации государственного учета использования потенциально опасных технологий;

– по согласованию порядка перемещения потенциально опасных технологий через таможенную границу государства.

Государственные органы исполнительной власти в соответствии с их компетенцией осуществляют:

– проведение государственной политики в сфере противодействия технологическому терроризму, обеспечения безопасности критически важных объектов, предупреждения и пресечения правонарушений в сфере оборота потенциально опасных технологий и контроля над ними;

– разработку проектов государственных программ и годовых планов деятельности в области обеспечения защиты от актов технологического терроризма и в области обеспечения безопасности критически важных объектов;

– разработку норм, правил и национальных стандартов в сфере противодействия технологическому терроризму;

– государственный учет использования потенциально опасных технологий и контроль над ними;

– разработку и реализацию мер по обеспечению антитеррористической защищенности критически важных объектов, оборота потенциально опасных технологий и средств транспортирования (перемещения) компонентов потенциально опасных технологий;

– разработку предложений по изменению законодательства в сфере противодействия технологическому терроризму;

– реализацию государственной системы реагирования на акты технологического терроризма;

– реализацию в пределах своей компетенции мер по обеспечению безопасности критически важных объектов;

– организацию подготовки кадров для государственных органов и иных организаций в сфере противодействия технологическому терроризму.

Администрация критически важных объектов несет ответственность за обеспечение безопасности оборота потенциально опасных технологий, а также за законность осуществления деятельности, связанной с их оборотом.

В указанных целях администрация критически важных объектов реализует следующие меры:

– обеспечивает антитеррористическую защищенность критически важных объектов;

– осуществляет внутренний учет процессов использования потенциально опасных технологий;

– обеспечивает физическую защиту оборота потенциально опасных технологий;

– допускает к непосредственной работе с потенциально опасными технологиями только лиц, прошедших специальное обучение, отвечающих квалификационным требованиям и не имеющих медицинских противопоказаний, а также прошедших в установленном порядке специальную проверку;

– обеспечивает конфиденциальность информации, бесконтрольное распространение которой может существенно понизить уровень антитеррористической защищенности критически важных объектов;

– заблаговременно информирует государственный регулирующий орган и национальный регистратор о планируемых сделках с использованием потенциально опасных технологий;

– заключает сделки только с организациями и учреждениями, имеющими разрешение (лицензию) на соответствующий вид деятельности;

– сообщает в государственный регулирующий орган и в правоохранительные органы обо всех ставших известными фактах несанкционированных действий с потенциально опасными технологиями.

4. Заключительные положения

Реализация настоящих Рекомендаций может осуществляться как путем подготовки и принятия специальных нормативных правовых актов в сфере противодействия технологическому терроризму, так и путем внесения необходимых изменений и дополнений в действующие нормативные правовые акты государств – участников СНГ.

Приняты на сорок втором
пленарном заседании
Межпарламентской Ассамблеи
государств – участников СНГ
(постановление № 42-7 от 16 апреля 2015 года)