

**П О С Т А Н О В Л Е Н И Е**

**Парламентской Ассамблеи**

**Организации Договора о коллективной безопасности**

|  |
| --- |
| **О проекте модельного закона ОДКБ**  **«Об информационном противоборстве терроризму и экстремизму»** |

|  |
| --- |
| Парламентская Ассамблея Организации Договора о коллективной безопасности п о с т а н о в л я е т:  1. Принять модельный закон ОДКБ «Об информационном противоборстве терроризму и экстремизму» (далее – модельный закон) (прилагается).  2. Направить указанный в пункте 1 настоящего постановления модельный закон в парламенты государств – членов ОДКБ для использования в работе по совершенствованию законодательства государств – членов Организации в соответствующей сфере.  3. Разместить модельный закон на официальном сайте и опубликовать в печатных материалах Парламентской Ассамблеи ОДКБ. |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| |  |  | | --- | --- | | **Председатель**  **Парламентской Ассамблеи ОДКБ** |  |  |  |  | | --- | --- | | **Москва**  **30 октября 2018 года**  **№ 11-3.3** |  | | **Описание: Описание: Описание: C:\Users\2\Pictures\2017-11-23\001.jpg** | **В. В. ВОЛОДИН** |

Принят

на одиннадцатом пленарном заседании

Парламентской Ассамблеи ОДКБ

30 октября 2018 года, постановление 11-3.3

**МОДЕЛЬНЫЙ ЗАКОН ОДКБ**

**«Об информационном противоборстве терроризму и экстремизму»**

Настоящий модельный закон ОДКБ (далее – Закон) определяет основы государственной политики в сфере информационного противоборства терроризму и экстремизму государств – членов ОДКБ (далее – государства), а также регламентирует общие вопросы организационного и правового обеспечения данной деятельности.

**Глава 1. ОБЩИЕ ПОЛОЖЕНИЯ**

Статья 1. **Правовая основа информационного противоборства терроризму и экстремизму**

Правовую основу информационного противоборства терроризму и экстремизму составляют конституция, настоящий Закон и иные нормативные правовые акты государства.

Отношения, возникающие в сфере информационного противоборства терроризму и экстремизму, затрагивающие интересы других государств либо международных организаций, регулируются соответствующими международными договорами. Если международным договором государства установлены иные правила, чем те, которые содержатся в настоящем Законе, то применяются правила международного договора.

Статья 2. **Основные понятия и их определения, применяемые в настоящем Законе**

В настоящем Законе используются следующие основные понятия и их определения:

*информационное противоборство терроризму и экстремизму* – деятельность субъектов информационного противоборства терроризму и экстремизму по оказанию комплексного воздействия с использованием специальных методов, способов и средств на террористическую и экстремистскую информационную среду в интересах искоренения терроризма и экстремизма, а также защиты легитимной информационной среды от террористического и экстремистского воздействия;

*информационная инфраструктура* – системы организационных структур, обеспечивающих информационное взаимодействие, информация в информационных системах, информационные системы, системы связи, защиты информации, телекоммуникации, радиоэлектронные средства и иные системы и средства, используемые в информационной сфере;

*легитимная информационная среда* – психика должностных лиц, общественных деятелей и населения государства, существующие в нем системы принятия решений, формирования общественного сознания, а также законная информационная инфраструктура;

*террористическая и экстремистская информационная среда* – психика лидеров терроризма и экстремизма, их сторонников, системы принятия ими решений и распространения террористического и экстремистского влияния, а также их информационная инфраструктура;

*информационно-техническое противоборство терроризму и экстремизму* – вид информационного противоборства терроризму и экстремизму, в котором главным объектом воздействия и защиты является информационная инфраструктура;

*информационно-психологическое противоборство терроризму и экстремизму* – вид информационного противоборства терроризму и экстремизму, в котором главным объектом защиты является психика должностных лиц, общественных деятелей и населения государства, существующие в нем системы принятия решений, формирования общественного сознания, а главным объектом воздействия – психика лидеров терроризма и экстремизма, их сторонников, системы принятия ими решений и распространения террористического и экстремистского влияния;

*информационная операция* – комплекс действий информационно-технического, информационно-психологического, разведывательного, оперативно-разыскного и иного характера по воздействию на террористическую и экстремистскую информационную среду и (или) защите легитимной информационной среды в условиях конкретизированных целей, объектов, сил, средств, способов и времени;

*информационное превосходство* ***–*** способность опережать противоборствующую сторону в сборе, обработке, использовании и распространении информации, а также установить и поддерживать превосходящий темп информационной операции, позволяющий доминировать во все время ее проведения и опережать возможные ответные акции.

Остальные понятия, используемые в настоящем Законе, понимаются в соответствии с их определениями, установленными модельными законами ОДКБ и национальным законодательством государств.

Статья 3. **Основные принципы информационного противоборства терроризму и экстремизму**

Информационное противоборство терроризму и экстремизму основывается на следующих принципах:

законности;

непрерывности;

превентивности;

соблюдения основных прав и свобод человека и гражданина;

приоритета мер предупреждения терроризма и экстремизма;

комплексности использования мер информационного противоборства терроризму и экстремизму;

неотвратимости наказания за осуществление террористической и экстремистской деятельности;

недопустимости уступок террористам и экстремистам;

правомерности причинения вреда террористам и экстремистам;

международного сотрудничества с другими государствами и международными организациями.

Статья 4. **Цели и задачи информационного противоборства терроризму и экстремизму**

Информационное противоборство терроризму и экстремизму осуществляется в целях:

разоблачения террористической и экстремистской идеологии, а также форм и методов ее распространения;

формирования в обществе обстановки нетерпимости к терроризму и экстремизму, неприятия террористических и экстремистских взглядов;

сокращения социальной базы поддержки терроризма и экстремизма;

повышения эффективности деятельности государственных органов, осуществляющих противодействие терроризму и экстремизму;

объединения усилий государственных структур и общественных институтов в вопросах профилактики терроризма и экстремизма;

достижения и удержания информационного превосходства в информационном противоборстве терроризму и экстремизму;

развития международного сотрудничества в данной сфере.

Для достижения указанных целей необходимо решить следующие задачи:

снизить информационно-психологическое воздействие идеологии терроризма и экстремизма на личность, общество и государство;

исключить доступ террористов и экстремистов к информации, которая может быть использована ими в преступных целях;

обеспечить упреждающий характер информационного воздействия на террористическую и экстремистскую информационную среду и защиты легитимной информационной среды;

не допустить использование террористами и экстремистами телекоммуникационных средств для подготовки и совершения преступлений, а также информационного обеспечения своей деятельности;

обеспечить профилактическое воздействие на население с целью недопущения вовлечения его представителей в террористическую и экстремистскую деятельность.

Статья 5. **Виды и основные направления информационного противоборства терроризму и экстремизму**

Информационное противоборство терроризму и экстремизму осуществляется в двух видах (информационно-техническое и информационно-психологическое противоборство) по следующим основным направлениям:

проведение разведки террористической и экстремистской деятельности в информационной сфере и разработка вариантов противодействия террористическому и экстремистскому воздействию на легитимную информационную среду;

воздействие на террористическую и экстремистскую информационную среду с целью искоренения терроризма и экстремизма;

защита легитимной информационной среды от террористического и экстремистского воздействия;

развитие технологической и производственной базы в области информационных технологий, повышение безопасности информационных и телекоммуникационных систем, систем и средств информатизации различных сфер деятельности;

совершенствование структуры обеспечения информационной безопасности;

подготовка специалистов в области информационного противоборства и обеспечения информационной безопасности;

взаимодействие с другими государствами и международными организациями по вопросам информационного противоборства терроризму и экстремизму.

**Глава 2. ОРГАНИЗАЦИОННЫЕ ОСНОВЫ ИНФОРМАЦИОННОГО ПРОТИВОБОРСТВА ТЕРРОРИЗМУ И ЭКСТРЕМИЗМУ**

Статья 6. **Государственная политика в сфере информационного противоборства терроризму и экстремизму**

В государстве осуществляется единая политика в сфере информационного противоборства терроризму и экстремизму, целью которой является обеспечение наиболее эффективного использования имеющихся ресурсов для достижения информационного превосходства над террористическими и экстремистскими организациями и недопущения использования ими информационных технологий в преступной деятельности.

Статья 7. **Система субъектов информационного противоборства терроризму и экстремизму**

Систему субъектов информационного противоборства терроризму и экстремизму составляют государственные органы (организации), органы местного самоуправления, общественные объединения и иные организации, а также физические лица, действующие в рамках полномочий, определенных законодательством государства. К ним относятся:

глава государства (правительство государства);

уполномоченный орган, координирующий деятельность по информационному противоборству терроризму и экстремизму (далее – уполномоченный орган);

государственные органы (организации), осуществляющие информационное противоборство терроризму и экстремизму;

органы местного самоуправления, общественные объединения и иные организации;

средства массовой информации;

физические лица.

Статья 8. **Полномочия главы государства (правительства государства)**

Глава государства (правительство государства):

определяет основные направления государственной политики в сфере информационного противоборства терроризму и экстремизму;

определяет уполномоченный орган;

определяет перечень и компетенцию государственных органов (организаций) в сфере информационного противоборства терроризму и экстремизму;

организует разработку и осуществление мер по предупреждению терроризма и минимизации и (или) ликвидации последствий проявлений терроризма;

устанавливает порядок взаимодействия государственных органов (организаций) в сфере информационного противоборства терроризму и экстремизму с уполномоченным органом;

организует выполнение обязательств государства по международным договорам в сфере информационного противоборства терроризму и экстремизму;

осуществляет иные полномочия, предусмотренные национальным законодательством.

Статья 9. **Уполномоченный орган**

Глава государства (правительство государства) в соответствии с национальным законодательством в целях координации деятельности государственных органов (организаций), общественных объединений и иных организаций в сфере информационного противоборства терроризму и экстремизму определяет уполномоченный орган.

Компетенция и порядок осуществления деятельности уполномоченного органа устанавливаются в соответствии с национальным законодательством и отражаются в специальном нормативном правовом акте, утверждаемом главой государства (правительством государства).

Статья 10. **Государственные органы (организации), осуществляющие информационное противоборство терроризму и экстремизму**

Информационное противоборство терроризму и экстремизму осуществляют государственные органы (организации) в пределах полномочий, предоставленных им законодательством государства.

Государственные органы (организации), осуществляющие информационное противоборство терроризму и экстремизму, решают стоящие перед ними задачи как самостоятельно, так и во взаимодействии друг с другом, а также с общественными объединениями и иными организациями. Формы взаимодействия определяются законодательством государства.

Формы взаимодействия между государственными органами (организациями), осуществляющими информационное противоборство терроризму и экстремизму, и государственными органами (организациями) иностранных государств определяются на основе соответствующих международных договоров.

Статья 11. **Участие органов местного самоуправления, общественных объединений и иных организаций в информационном противоборстве терроризму и экстремизму**

Органы местного самоуправления, общественные объединения и иные организации участвуют в информационном противоборстве терроризму и экстремизму в тесном взаимодействии с государственными органами (организациями), осуществляющими информационное противоборство терроризму и экстремизму, в соответствии с законодательством государства.

Статья 12. **Средства массовой информации в информационном противоборстве терроризму и экстремизму**

Средства массовой информации осуществляют свою деятельность в целях формирования в обществе неприятия террористических и экстремистских идей, а также недопущения использования средств массовой информации террористическими и экстремистскими организациями для информационной поддержки своей деятельности.

Руководители средств массовой информации обязаны принимать меры к тому, чтобы материалы, подготовленные в руководимых ими органах, не обеспечивали информационную поддержку террористической и экстремистской деятельности.

Информация, полученная работниками средств массовой информации, свидетельствующая о готовящихся преступлениях террористической или экстремистской направленности либо являющаяся доказательством такой деятельности, должна незамедлительно передаваться государственным органам (организациям), осуществляющим борьбу с терроризмом и экстремизмом.

Работники средств массовой информации, допустившие нарушения своих обязанностей в части содействия информационному противоборству терроризму и экстремизму, несут ответственность в соответствии с законодательством государства. В отношении средства массовой информации, работники которого систематически (два раза и более) нарушали требования законодательства об информационном противоборстве терроризму и экстремизму, может быть наложен запрет на осуществление деятельности в порядке, предусмотренном законодательством государства.

Статья 13. **Физические лица**

Физические лица на добровольных началах участвуют в решении задач информационного противоборства терроризму и экстремизму в форме оказания содействия государственным органам (организациям), осуществляющим информационное противоборство терроризму и экстремизму.

Порядок привлечения физических лиц к решению задач информационного противоборства терроризму и экстремизму определяется законодательством государства.

Физические лица также вправе осуществлять не нарушающие законодательства государства инициативные действия по прекращению или затруднению функционирования систем управления, принятия решений и финансирования террористической и экстремистской деятельности, а также по ее дезорганизации с использованием программно-технического воздействия, распространению в сегментах Интернета антитеррористической информации, пропаганде несостоятельности террористической и экстремистской идеологии.

**Глава 3. СИСТЕМА МЕР ИНФОРМАЦИОННОГО ПРОТИВОБОРСТВА ТЕРРОРИЗМУ И ЭКСТРЕМИЗМУ**

Статья 14. **Информационные и информационно-аналитические меры**

Информационными и информационно-аналитическими мерами противоборства терроризму и экстремизму являются:

добывание достоверной, полной и своевременной информации о террористическом и экстремистском воздействии на легитимную информационную среду, об условиях и угрозах такого воздействия;

всесторонний анализ достоверных данных о силах, средствах, формах и методах террористической и экстремистской деятельности в информационной сфере;

прогнозирование изменения условий информационного противоборства терроризму и экстремизму с целью разработки вариантов воздействия на террористическую и экстремистскую информационную среду и защиты легитимной информационной среды, а также расчет их последствий;

подготовка информационно-пропагандистских материалов и информационное обеспечение информационных операций.

Статья 15. **Меры воздействия на террористическую и экстремистскую информационную среду**

Мерами воздействия на террористическую и экстремистскую информационную среду в процессе информационного противоборства терроризму и экстремизму являются:

проведение специальных мероприятий по прекращению или затруднению функционирования систем управления, принятия решений и финансирования террористической и экстремистской деятельности, а также по ее дезорганизации;

применение в отношении террористической и экстремистской информационной инфраструктуры наступательных средств программно-технического воздействия;

физическое разрушение объектов террористической и экстремистской информационной инфраструктуры;

антитеррористическая информационная экспансия в сегментах Интернета, используемых в террористических и экстремистских целях, с применением соответствующих способов информационно-психологического воздействия как на нейтральных пользователей, так и на лидеров террористов и экстремистов, их сторонников;

осуществление информационно-психологического влияния на лидеров терроризма и экстремизма, а также их сторонников с целью побуждения их к совершению действий, выгодных с точки зрения противоборства терроризму и экстремизму;

пропаганда несостоятельности террористической и экстремистской идеологии в разрешении социальных конфликтов, нацеленная на склонение к отказу от такой деятельности лиц, ее разделяющих.

Статья 16. **Меры защиты легитимной информационной среды**

Мерами защиты легитимной информационной среды в процессе информационного противоборства терроризму и экстремизму являются:

обеспечение информационной безопасности легитимной информационной инфраструктуры;

использование программно-технических средств проверки законности доступа к информационным ресурсам, идентификации пользователей, регистрации всех их действий (с возможностью оперативного и последующего анализа), обеспечивающих необходимый уровень конфиденциальности;

предотвращение кибератак против автоматизированных систем управления технологическими процессами и критически важной инфраструктуры, снижение их уязвимости, минимизация ущерба и времени восстановления в случае нарушения их функционирования;

противодействие преступным посягательствам террористической и экстремистской направленности против легитимной информационной среды, а также в сфере информационной безопасности государства посредством оперативно-разыскной, уголовно-процессуальной и иной правоохранительной деятельности;

установление и исполнение запретов (уголовных, административных) на совершение действий террористического и экстремистского характера, направленных против легитимной информационной среды;

введение и контроль исполнения организатором распространения информации в Интернете, в том числе реализующим функции организатора сервиса обмена мгновенными сообщениями, а также оператором связи, оказывающим услуги по предоставлению доступа к Интернету, обязанности по ограничению (блокированию) доступа к информации террористического или экстремистского характера в Интернете, распространение которой в государстве запрещено, либо к содержащему ее информационному ресурсу;

определение условий по ограничению доступа пользователей Интернета к информации террористического или экстремистского характера, запрещенной для распространения, и обеспечение их реализации;

информационно-пропагандистские действия, направленные на формирование у населения государства неприятия терроризма и экстремизма.

Статья 17. **Организационно-управленческие меры**

Организационно-управленческими мерами информационного противоборства терроризму и экстремизму являются:

создание, определение компетенции и регулирование деятельности специальных организационных структур для осуществления информационного противоборства терроризму и экстремизму;

определение порядка участия в информационном противоборстве терроризму и экстремизму государственных органов (организаций), общественных объединений и иных организаций, а также граждан;

определение порядка создания и применения средств информационно-технического и информационно-психологического воздействия на террористическую и экстремистскую информационную среду;

разработка и обеспечение эффективного функционирования организационно-правового механизма отнесения информации к сведениям террористического или экстремистского характера, распространение которых запрещено;

организация системы подготовки кадров для сферы информационного противоборства терроризму и экстремизму;

разработка программ информационного противоборства терроризму и экстремизму и обеспечение их реализации;

организация системы психологической помощи и ресоциализации для лиц, вовлеченных с помощью информационных технологий в террористическую и экстремистскую деятельность и принявших решение прекратить свое участие в такой деятельности;

обеспечение эффективного взаимодействия всех участников информационного противоборства терроризму и экстремизму как на внутригосударственном, так и на международном уровнях.

**Глава 4. МЕЖДУНАРОДНОЕ СОТРУДНИЧЕСТВО В СФЕРЕ ИНФОРМАЦИОННОГО ПРОТИВОБОРСТВА ТЕРРОРИЗМУ**

**И ЭКСТРЕМИЗМУ**

Статья 18. **Правовая основа международного сотрудничества в сфере информационного противоборства терроризму и экстремизму**

Правовую основу международного сотрудничества в сфере информационного противоборства терроризму и экстремизму составляют международные договоры, а также национальное законодательство государств.

Статья 19. **Цели международного сотрудничества в сфере информационного противоборства терроризму и экстремизму**

Международное сотрудничество в сфере информационного противоборства терроризму и экстремизму осуществляется в целях:

выработки согласованной политики и объединения усилий государств в вопросах информационного противоборства терроризму и экстремизму;

исключения практики применения двойных стандартов в борьбе с терроризмом и экстремизмом;

повышения эффективности взаимодействия государственных органов (организаций), осуществляющих информационное противоборство терроризму и экстремизму;

совершенствования правовой базы международного сотрудничества в сфере информационного противоборства терроризму и экстремизму;

гармонизации национального законодательства государств в сфере информационного противоборства терроризму и экстремизму.

Статья 20. **Основные направления и формы международного сотрудничества в сфере информационного противоборства терроризму и экстремизму**

Международное сотрудничество в сфере информационного противоборства терроризму и экстремизму осуществляется по следующим основным направлениям:

договорно-правовое;

научно-информационное;

научно-техническое;

организационное;

профилактическое;

образовательное.

Основными формами международного сотрудничества в сфере информационного противоборства терроризму и экстремизму являются:

оказание взаимной правовой помощи в соответствии с международными договорами государств;

совершенствование правового обеспечения информационного противоборства терроризму и экстремизму;

обмен информацией, результатами научных исследований и опытом практической деятельности в данной сфере;

проведение совместных научных и научно-технических исследований;

проведение взаимных консультаций по проблемам международного сотрудничества в сфере информационного противоборства терроризму и экстремизму;

организация научных семинаров и иных научных мероприятий в сфере информационного противоборства терроризму и экстремизму;

оказание технического содействия в проведении информационно-пропагандистских мероприятий;

обмен техническими разработками в сфере информационного противоборства терроризму и экстремизму;

проведение совместных информационно-пропагандистских мероприятий;

взаимодействие государственных органов (организаций), осуществляющих информационное противоборство терроризму и экстремизму, по вопросам совершенствования их деятельности;

устранение причин и условий, способствующих информационной агрессии террористических и экстремистских организаций;

совместная подготовка и переподготовка кадров, повышение квалификации специалистов и стажировки представителей государственных органов (организаций), осуществляющих информационное противоборство терроризму и экстремизму;

обмен методическими разработками в сфере информационного противоборства терроризму и экстремизму.

**Глава 5. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ**

Статья 21. **Контроль за информационным противоборством терроризму и экстремизму**

Контроль за информационным противоборством терроризму и экстремизму осуществляет уполномоченный орган государства.

Статья 22. **Надзор за законностью информационного противоборства терроризму и экстремизму**

Надзор за исполнением законодательства об информационном противоборстве терроризму и экстремизму осуществляют генеральный прокурор государства и подчиненные ему прокуроры в пределах своей компетенции.

Статья 23. **Ответственность за нарушение законодательства в сфере информационного противоборства терроризму и экстремизму**

Лица, виновные в нарушении законодательства в сфере информационного противоборства терроризму и экстремизму, несут гражданскую, административную, уголовную и иную ответственность в соответствии с законами государства.