ПРОБЛЕМЫ УГОЛОВНОГО ПРАВА И КРИМИНОЛОГИИ

УДК 343

О СОВЕРШЕНСТВОВАНИИ МЕР ПРОТИВОДЕЙСТВИЯ ПРИМЕНЕНИЮ ТЕРРОРИСТАМИ НОВЫХ ТЕХНОЛОГИЙ

Абдулатипов А.М., Дагестанский государственный университет, г. Махачкала, Российская Федерация, tta-msshm@yandex.ru

Статья посвящена исследованию мер противодействия использованию террористами достижений науки, техники и новейших технологий в преступных целях. В работе отражены технологии, представляющие наиболее существенную террористическую угрозу, проведён анализ и обобщение существующего опыта противодействия использованию этих технологий для совершения терактов. Выделены основные мероприятия, направленные на противодействие кибертерроризму на международном, федеральном уровне, а также наиболее действенные формы превенции кибертерроризма в регионе. На основе исследования автор сделал ряд выводов и предложений, имеющих теоретическое и практическое значение.

Ключевые слова: кибертерроризм, информационное пространство, новые технологии, безопасность, противодействие.

DOI: 10.21779/2224-0241-2020-36-4-123-129

UDC 343

ABOUT IMPROVEMENT OF MEASURES TO COUNTER TERRORISTS USE NEW TECHNOLOGIES

Abdulatipov A.M., Dagestan State University, Makhachkala, Russian Federation, tta-msshm@yandex.ru

The article is devoted to the study of measures to counter terrorists use achievement of science and new technologies for criminal purposes. The article reflects the technologies that represent the most significant terrorist threat. It also analyzes and summarizes the existing experience of countering the use of these technologies for terrorist attacks. The article also highlights the main activities aimed at countering cyberterrorism at the international and Federal levels, as well as the most effective forms of prevention of cyberterrorism in the region. Based on the study, the author made a number of conclusions and proposals of theoretical and practical importance.

Key words: cyberterrorism, information space, new technology, security, countering.

DOI: 10.21779/2224-0241-2020-36-4-123-129

Терроризм, как любое негативное социальное явление испытывает постоянные изменения. В связи с возникшими на современном этапе потенциальными возможностями использования при совершении преступлений новейших информационных технологий, телекоммуникационных систем и средств, киберпространства, появился новый наиболее опасный вид терроризма, который одни называют кибертерроризмом либо электронным терроризмом, другие – информационным терроризмом.

На заседании Совета безопасности России Президент РФ отметил, что проблема (кибертерроризма) в последнее время приобрела глобальный характер. Для России её решение имеет стратегическое значение. А информационная безопасность является одним из важнейших факторов обеспечения суверенитета и национальной безопасности.

Уровень угроз в информационном пространстве повышается [1].

Кибертерроризм представляет собой серьёзную угрозу для человечества, сравнимую с ядерным, бактериологическим и химическим оружием; причем степень этой угрозы в силу своей новизны не до конца ещё осознана и изучена. Опыт мирового сообщества в этой области со всей очевидностью свидетельствует о несомненной уязвимости любого государства, тем более что кибертерроризм не имеет государственных границ, кибертеррорист способен в равной степени угрожать информационным системам, расположенным практически в любой точке земного шара [2].

Как показывает современная практика, международные террористические организации (далее – МТО), включая «Аль-Каиду», «ИГ» и другие активно используют киберпространство для плани-

рования и организации экстремистской и террористической деятельности, связи и обмена информацией, ведения пропаганды, вербовки новых членов и размещения инструкции о методах и способах изготовления взрывных устройств, ведения подрывной деятельности, рекрутирования в свои ряды хакеров, из которых нередко формируют собственные «киберотряды», которые могут планировать и осуществить кибератаки на потенциально опасные инфраструктуры в целях провоцирования техногенных аварий и экологических катастроф.

Так, Рамзи Юзеф, организовавший взрыв Всемирного торгового центра в Нью-Йорке 11 сентября 2001 г., получал по Интернету зашифрованные инструктивные послания от Усамы бен Ладена. Таким образом, в конце XX века появилось совершенно новое явление в сфере информационных технологий: компьютерный или кибертерроризм, использующий для достижения своих преступных целей компьютеры, электронные сети и самые современные информационные технологии [3].

Подготовка к совершению терактов требует активного использования информационных ресурсов, в том числе и в целях обеспечения широкой средовой поддержки преступных акций. Для этого, например, ещё в конце прошлого и начале нынешнего столетия международными террористами, действовавшими в Чеченской Республике, было сформировано специальное подразделение. Созданное сепаратистским идеологом М. Удугвым так называемое «Информационное агентство «Кавказ-центр» открыло одноименный сайт в сети Интернет. Это агентство занималось распространением дезинформации об успехах террористов и больших потерях федеральных сил с целью сформировать у мировой общественности и руководства иностранных государств негативное отношение к России.

В этой преступной акции использовалось более 100 финансируемых террористами сайтов на русском, английском, арабском, французском и других языках. Лидерами террористов были созданы информационные центры в Азербайджане, Грузии, Украине, Литве, Финляндии, Турции и Польше. Через эти структуры распространялись заведомо ложные сведения, призванные создать в общественном сознании Запада мифы о «зверствах русских солдат в отношении мирного населения», «гуманитарной катастрофе на Северном Кавказе». При этом они руководствовались принципом «чем чудовищнее ложь, тем быстрее в нее поверят» (к примеру, провокационное заявление Мовлади Удугова о причастности дагестанских граждан, погибших на атомоходе «Курск», к взрыву атомной подводной лодки) [4].

Как отмечают учёные, в настоящее время наиболее существенную террористическую угрозу представляют следующие технологии: виртуальные игровые технологии в области рекрутирования; системы киберплатежей на анонимной основе для финансовых трансфертов; многопользовательские онлайн-игры для обучения и коммуникации;

технологии высококачественного копирования и манипуляции текстом и изображениями для изготовления поддельных документов и продуктов; технологии деперсонификации пользователя в среде электронных коммуникаций для осуществления скрытных действий и ухода от преследования; технологии глобальной, защищенной, многофункциональной мобильной коммуникации для тех же целей; фальсификация видео и аудио сообщений от имени известных публичных фигур для дестабилизации обстановки; технологии электронного перехвата контроля над информационными каналами в тех же целях и т.д. [5].

Лидеры террористических организаций стремились ускоренно овладеть перечисленными технологиями и их прикладными приложениями.

Вместе с тем, в течение длительного времени государственные, в том числе правоохранительные органы не уделяли должного внимания данному процессу, в связи с чем было допущено серьёзное отставание в этом направлении. А вербовщики и агитаторы террористических структур, воспользовавшись этим и фактически постоянным присутствием молодежи в социальных сетях, развернули в Интернете активную деятельность по оправданию экстремизма и терроризма, героизации членов незаконных вооруженных формирований, демонстрации «лесной романтики» путём размещения в социальных сетях фотографий боевиков, видеозаписей «красивой лесной жизни», радикальных лозунгов, призывов, умело подготовленных и вырванных из контекста выдержек из Корана и т.д.

Несмотря на изменения в Федеральном законе №149-ФЗ «Об информации, информационных технологиях и о защите информации», в части представления возможности блокировки экстремистского контента в сети Интернет, а также введения ответственности за публичные призывы к осуществлению действий, направленных на нарушение территориальной целостности РФ, в том числе совершенные с использованием средств массовой информации и информационно-телекоммуникационных сетей, включая Интернет, эффективность работы субъектов профилактики в данной сфере не адекватна сложившейся ситуации.

В частности, в РФ это обусловлено недостатками в деятельности компетентных органов по выявлению и блокированию террористических и экстремистских материалов в сети «Интернет»; организации взаимодействия между соответствующими структурами по вопросам своевременного проведения экспертизы указанных материалов, что часто приводит к затягиванию сроков окончательного закрытия доступа к противоправным ресурсам; антитеррористической защищенности отдельных категорий объектов (транспортной инфраструктуры – нарушения пропускного и внутриобъектового режимов, отсутствие оценки уязвимости объектов и предоставление ее результатов в Федеральное дорожное агентство, упущения в подготовке и аттестации соответствующих специали-

стов; объектов здравоохранения – отсутствие регламентирующих документов по антитеррористической защищённости, упущения в инженерно-техническом оснащении объектов; топливно-энергетического комплекса – занижение категорий объектов, нарушения в проектной документации [6].

Об этом свидетельствует и уголовная статистика. Только в 2018 году, по данным ИЦ МВД по РД, на территории Республики Дагестан зарегистрировано 447 (531) преступлений террористической направленности (по фактам оказания пособнической помощи членам НВФ и участия за рубежом в составе МТО) и 75 (87) преступлений экстремистского характера.

Таким образом, масштабное развитие информатизации и информационных технологий приносит не только огромные позитивные изменения во всех сферах жизнедеятельности нашего общества, но и потенциальную возможность их использования в новых преступных целях.

Конвенция Совета Европы от 2001 г. «О киберпреступности» [7], обязало каждое государств-участника создать внутреннюю законодательную базу, обязывающую, во-первых, предоставлять органам, осуществляющим противодействие кибертерроризму, полномочия по выемке компьютерных систем, их частей или носителей; изготовлению и конфискации копий данных; обеспечению целостности и сохранности данных, относящихся к делу; уничтожению или блокировке данных, находящихся в компьютерной системе; во-вторых, Интернет-провайдеров – проводить сбор и фиксацию или перехват необходимой информации с помощью имеющихся технических средств, а также способствовать в этом компетентным органам.

18 января 2013 г. в Гааге открыли Европейский центр по борьбе с киберпреступностью [8] в целях сбора и обработки данных по киберпреступности; подготовки квалифицированных кадров; экспертной оценки киберугроз; разработки и внедрения передовых форм и методов профилактики и расследования киберпреступлений.

В СНГ создан Антитеррористический центр (АТЦ), в составе которого сформирован и эксплуатируется межгосударственная автоматизированная информационная система – Специализированный банк данных АТЦ СНГ [9], в котором накапливаются сведения о международных террористических и иных экстремистских организациях, их лидерах, причастных к ним лицах; состоянии, динамике и тенденциях распространения международного терроризма, а также о неправительственных структурах и лицах, оказывающих поддержку международным террористам; массивы, содержащие сведения в отношении лиц, объявленных в международный розыск по подозрению в совершении преступлений террористического характера; юридических и физических лиц, финансирующих террористические и экстремистские организации; лиц и организаций, подозреваемых в причастности

к совершению актов терроризма с использованием террористов-смертников.

В Российской Федерации наиболее важное место в этой системе занимают соответствующие подразделения Национального антитеррористического комитета, Федерального оперативного штаба, Антитеррористических комиссий и оперативных штабов в субъектах РФ. В структурах Федеральной службы безопасности, Министерства внутренних дел, Министерства обороны, Роскомнадзора и ряда других ведомств созданы соответствующие подразделения по противодействию информационному терроризму.

Указом Президента РФ от 15 января 2013 г. №31 на ФСБ России возложены полномочия по созданию государственной системы обнаружения, предупреждения и ликвидации компьютерных атак на информационные ресурсы РФ, информационные системы и информационно-телекоммуникационные сети, находящиеся на территории РФ и в дипломатических представительствах и консульских учреждениях РФ за рубежом.

В составе Генерального штаба ВС России приказом министра обороны от 14 января 2014 года созданы войска информационных операций [10].

Также принята Стратегия противодействия экстремизму в Российской Федерации до 2025 года (утв. Президентом РФ 28.11.2014 г. № Пр-2753).

В настоящее время на стадии принятия находится новый Федеральный закон об устойчивом функционировании Рунета (Российского сегмента сети «Интернет»).

Как известно, сущность противодействия кибертерроризму заключается в обеспечении эффективной защиты информационных ресурсов и потенциально опасных объектов от кибератак, а также использовании специальных средств и способов воздействия на информационные ресурсы террористических структур.

В связи с этим, в качестве основных задач государственной политики в сфере противодействия кибертерроризму рассматриваются: создание единой государственной системы мониторинга в сфере противодействия экстремизму и терроризму; совершенствование законодательства РФ и правоприменительной практики, а также консолидация усилий федеральных органов государственной власти, органов государственной власти субъектов РФ, органов местного самоуправления, институтов гражданского общества и организаций в данной сфере; организация в средствах массовой информации, информационно-телекоммуникационных сетях, информационного сопровождения их деятельности, а также реализация эффективных мер информационного противодействия распространению идеологии экстремизма и терроризма; разработка и осуществление комплекса мер по повышению эффективности профилактики, выявления и пресечения террористических и экстремистских проявлений.

В целях противодействия различного рода террористическим и экстремистским проявлениям,

в том числе оперативного реагирования на пропаганду экстремизма в сети Интернет, Председатель СКР А. Бастрыкин предлагает предусмотреть внесудебный порядок включения информации в федеральный список экстремистских материалов, а также блокировки доменных имен сайтов, распространяющих данную информацию [11].

В связи с наличием особенностей противодействия кибертерроризму на международном, федеральном и региональном уровнях, важное практическое значение имеет разработка мер для каждого из них отдельно.

Так, на основе анализа и обобщения существующего опыта антитеррористической деятельности А. Королёв [12], выделяет следующие основные мероприятия, направленные на противодействие кибертерроризму. **На международном уровне** он выделяет: организацию межгосударственного сотрудничества в работе международных организаций, общественных комитетов и комиссий в проектах развития мировых информационных сетей; активное участие в разработке международного законодательства и нормативно-правового обеспечения функционирования мировых открытых сетей; создание единого антитеррористического пространства стран-союзников; разработку научно-методического обеспечения по пресечению транснациональных (трансграничных) террористических атак с использованием глобальных информационных сетей, выработка единого понятийного аппарата, шкалы оценки киберугроз и их последствий; выработку механизмов взаимного информирования о широкомасштабных компьютерных атаках и крупных инцидентах в киберпространстве, а также способов совместного реагирования на угрозы кибертерроризма; унификацию национальных законодательств в сфере защиты критической инфраструктуры от кибертерроризма.

На федеральном уровне можно применить следующие меры: организацию мониторинга и прогнозирования потребностей экономических и других структур в различных видах информационного обмена через международные сети; координацию мер государственных и негосударственных ведомств по предотвращению угроз информационной безопасности в открытых сетях; разработку государственной программы совершенствования информационных технологий, обеспечивающих подключение национальных и корпоративных сетей к мировым открытым сетям при соблюдении требований безопасности информационных ресурсов; совершенствование технологий своевременного обнаружения и нейтрализации несанкционированного доступа к информации; разработку национального законодательства в части правил обращения с информационными ресурсами, регламента прав, обязанностей и ответственности пользователей открытых мировых сетей; организацию системы комплексной подготовки и повышения квалификации массовых пользователей и специалистов по информационной безопасности для работы в мировых информационных сетях.

Учёные [13] также предлагают использование методики противодействия киберугрозам по следующим четырем направлениям: практики, предполагающие отказ в доступе террористам к новым технологиям посредством прямых (нормативных) ограничений на распространение определенного технологического оборудования либо иного противодействия террористическим группам в получении доступа к конкретной технологии; практики, предполагающие создание препятствий в применении технологии (глушение каналов связи или вывод из строя террористических веб-сайтов посредством вредоносных программных продуктов и т. д.); практики, предполагающие скрытую эксплуатацию технологических уязвимостей и дефектов для получения критически значимой информации, облегчающей осуществление мер прямого действия против террористов (аресты, акции возмездия и т.д.); практика, предполагающая непротодействие. Последний вариант может быть достаточно рациональным в случаях, когда есть основания ожидать незначительный эффект от применения террористами новых технологий в своей деятельности. Только комплексное использование перечисленных практик противодействия кибертерроризму может иметь максимальный практический эффект.

Вместе с тем, оценивая криминальную угрозу от информатизации на федеральном и международном уровне, следует также учитывать её **особенности в регионах** России, в которых она проявляется с определённой спецификой, что необходимо для выработки эффективной системы нейтрализации этих угроз на региональном уровне.

Так, если рассмотреть данную проблему на примере Дагестана, то здесь прослеживается своя специфика, которая, как и в других республиках Северного Кавказа, обусловлена широкой распространённостью использования компьютерных технологий в экстремистских и террористических целях.

Эта специфика обусловлена, во-первых, наличием в составе МТО большого количества выходцев из Дагестана. По данным ЦПЭ МВД по РД, установлено и объявлено в розыск 1529 жителей Дагестана, участвующих в МТО, задержано при попытке выезда в Сирию для участия в составе МТО 85 человек. Необходимо отметить, что лидеры МТО стремятся вовлекать в террористическую сеть лиц с высоким потенциалом и профессиональным уровнем в сфере информатики и информационных технологий. Во-вторых, значительно повышает уровень террористических угроз стремление лидеров МТО организовать в Республике Дагестан деятельность своих сторонников путем создания автономных террористических групп, т.н. «спящих ячеек». Об этом свидетельствует то, что только в 2018 году, по данным ЦПЭ МВД по РД, выявлены и ликвидированы 7 таких ячеек в городах Хасавюрт, Дербент, Махачкала, Каспийск и Буйнакск, при оказании вооруженного сопротивления ликвидированы 15 и задержаны 14 членов ячеек и их пособников, изъято большое количество оружия и

боеприпасов, предотвращены подготавливаемые им террористические акции. В структуре этих ячеек состоят молодые люди, способные осваивать новые технологии, о которых ранее не имели представления, и быстро адаптировать их для совершения новых видов преступлений. Для этого им не нужны большие затраты, так как компьютерная техника постоянно дешевеет. Об этом свидетельствует также постоянно растущее число пользователей социальных сетей в республике, в первую очередь, Интернет-сети. В-третьих, наличие широкой пособнической базы из членов семей террористов; по данным ЦПЭ МВД по РД, установлено 579 вдов убитых террористов, 1138 семей, в которых воспитываются 2383 несовершеннолетних детей, из них 228 детей, находящихся с родителями в Сирийской Арабской Республике. В-четвертых, сохраняющаяся потенциальная возможность, хотя пока еще немногочисленного, но в дальнейшем массового возвращения в республику террористов, находящихся в составе международных террористических организаций, которые хорошо усвоили компьютерные технологии и имеют опыт ведения боевых действий, в том числе в условиях населенного пункта. По данным правоохранительных органов, в республике задержано 131 участник МТО, возвратившихся из Сирии, из них в 2018 год – 11 человек. Это может вполне реально вызвать увеличение компьютеризации террористических ячеек в республике и на основании чего можно прогнозировать рост кибертерроризма. В-пятых, высокий уровень безработицы, отсутствие реального сектора высокотехнологичной экономики и, связанная с этим, неадекватная востребованность специалистов в области информатики в социально – экономической и иной сфере жизнедеятельности способствует оттоку молодых специалистов в криминальные структуры, особенно в террористические и экстремистские. Тем более что молодежь является самой многочисленной социально-демографической группой в Республике Дагестан. По данным Всероссийской переписи населения 2010 года [14], в республике проживало 951122 молодых людей в возрасте от 14 до 30 лет, что составляет почти 33% общего числа ее жителей. В то же время, низкий социальный статус, отсутствие социальных навыков и профессионального опыта, возрастные особенности делает ее наиболее уязвимой группой населения.

Такая же тенденция наблюдается и на мировом уровне. Как отмечает В. Д. Бородин [15, с. 15], с использованием новейших технологий и средств при совершении преступлений, таких как спутниковая связь, использование киберпространства, появляется новая генерация личности – на мировой арене активизируется ювенотерроризм. Учитывая максималистские взгляды молодежи, можно легко развить любую фанатичную идею до абсолюта. Эта идея может быть представлена в виде секты (Аум-Сенрикё), спортивного клуба («Белый лотос»), спецлагеря (учреждения в Палестине для подготовки малолетних террористов-камикадзе).

Только в 2018 году, по данным ИЦ МВД по РД, на территории республики правоохранительными органами выявлено 76 (для сравнения – 84 за прошлый год) преступлений, связанных с распространением террористической и экстремистской идеологии в сети Интернет, совершённых данной категорией лиц. В Роскомнадзор направлено 740 материалов на блокировку экстремистских Интернет-ресурсов (заблокировано 235).

В целях адекватного противодействия информационному терроризму и экстремизму, в республике приняты организационные меры. На основании Директивы ФОШ от 18.08.2011 года №8 и Распоряжения МВД РФ от 29.08.2011 года №375, создана Оперативная группа МВД России по противодействию террористической и экстремистской идеологии, в том числе в сфере высоких технологий, с местом дислокации в г. Махачкале. Данной группе вменены следующие направления деятельности: осуществление мониторинга в сети Интернет; документирование преступной деятельности лиц и организаций, занимающихся распространением террористической и экстремистской идеологии, выявленных в ходе мониторинга, или по полученной из иных каналов информации; информационно-пропагандистские мероприятия; ограничение доступа к экстремистским ресурсам.

В структуре ЦПЭ МВД по РД создан специализированный отдел по информационному противодействию экстремизму, основными задачами которого являются: мониторинг, анализ и прогнозирование экстремистских угроз; выявление в сети Интернет пользователей и веб-страниц, на которых ведется пропаганда и поддержка экстремистских идей, оправдание терроризма, призывов к нарушению территориальной целостности России; оказание информационного противодействия распространению идеологии экстремизма. В социальных сетях «Инстаграмм», «ВКонтакте», «Фейсбук», «Одноклассники», «Твиттер», «Мой мир» созданы специализированные администрируемые группы под названием «Антитеррор – Дагестан», «Точка кипения», «Дагестан в событиях» для проведения информационно-пропагандистских мероприятий. На сайтах «Кавполит», «Годекан», «Оперативная линия», «Точка кипения», «Дагпресс» и на российском новостном блоге обмена ссылками «Вотт» и др., размещены материалы по информированию населения о преступниках, находящихся в розыске за совершение преступлений экстремисткой направленности и террористического характера, их пособниках, вербовщиках и идеологах.

В этих же целях в Республике Дагестан разработаны и реализуются нормативные правовые акты и государственные программы: Закон Республики Дагестан «О профилактике экстремистской деятельности» от 04.04.2016 г. №20; Постановление Правительства РД «Об организации деятельности органов исполнительной власти в области противодействия терроризму» от 14 марта 2017 года №61; государственная программа «Взаимодействие с религиозными организациями и их государствен-

ная поддержка на 2017-2019 годы», утвержденная постановлением Правительства РД от 28.12.2016 года №408; приказ МВД по РД от 14.03.2014 года № 464 «О совершенствовании деятельности органов внутренних дел в высших и средних специальных учебных заведениях РД» (в новой редакции – от 17.08.2018 г. №1117), во исполнение которого созданы рабочие группы по противодействию распространению экстремизма и терроризма в учебных заведениях республики; распоряжения МВД по РД от 20.09.2015 года № 26/128 «О дополнительных мерах по предотвращению вовлечения несовершеннолетних в террористическую деятельность и недопущению распространения радикальной идеологии в молодежной среде»; от 08.04.2014 года №26/52 «О профилактике распространения экстремистской идеологии в школьных и дошкольных учебных заведениях РД»; от 28.12.2014 года №52/1814 «О проведении профилактической работы с семьями членов бандподполья»; от 30.11.2015 года № 26/152 «О мерах по профилактике и недопущению распространения экстремистской идеологии в общеобразовательных учебных заведениях»; от 18.01.2018 года № 32/279 «О совершенствовании оперативно-розыскной и профилактической работы в религиозных учебных заведениях РД» и др.

На основе исследования и изучения опыта противодействия кибертерроризму в России можно выделить наиболее действенные формы его профилактики в регионе:

- разработка проектов нормативных правовых актов и программных документов, принятие управленческих решений в сфере противодействия кибертерроризму с учетом стратегии развития новейших технологий;

- в соответствии с Федеральным законом от 23.06.2016 года №182-ФЗ «Об основах системы профилактики правонарушений в РФ» обновление системы профилактики терроризма, определить зону ответственности всех субъектов; совершенствовать оперативно-профилактический контроль за подучётными лицами, а также отбывшими наказание и амнистированными по статьям террористической направленности, членами семей убитых террористов;

- принятие на региональном и муниципальном уровнях соответствующих целевых программ, предусматривающих формирование системы профилактики экстремизма и терроризма в информационной сфере;

- вовлечение институтов гражданского общества, общественных организаций, бизнеса в процесс осуществления антитеррористической пропаганды в блогосферах и социальных сетях;

- координация действий правоохранитель-

ных органов, органов государственной власти, органов местного самоуправления, политических партий, общественных и религиозных объединений по пресечению кибертерроризма;

- реализовать с использованием цифровых технологий комплекс мер, направленный на выявление и пресечение на ранней стадии деятельности автономных групп (так называемых «спящих ячеек»), создаваемых в регионе приверженцами религиозного экстремизма, а также проповедников и приверженцев идей радикального ислама, ксенофобии и сепаратизма;

- выявление и устранение источников и каналов финансирования террористической и экстремистской деятельности в сетевых ресурсах;

- обеспечение подготовки сотрудников правоохранительных органов и получения ими дополнительного профессионального образования по утвержденным в установленном порядке типовым учебным программам по вопросам выявления, пресечения, раскрытия, профилактики и квалификации террористических проявлений с использованием высоких технологий;

- мониторинг общественно-политических и социально-экономических процессов, обсуждаемых в сети «Интернет», для принятия контрпропагандистских мер информационного противоборства;

- выявление экстремистских ресурсов в целях ограничения доступа к экстремистским сайтам, документирования и закрытия ресурса;

- мониторинг «Федерального списка экстремистских материалов Министерства юстиции РФ» и проверка Интернет-ресурсов, включенных в него на доступность, вынесение предписаний провайдером Интернет, на ограничение доступа пользователей к таким ресурсам;

- совершенствование процесса мониторинга, сбора, накопления, анализа информации, представляющей оперативный интерес, выявления лиц, занимающихся распространением экстремистской идеологии в интернет-ресурсах, методики обследования Интернет-сайтов и проведения лингвистических и этноконфликтологических исследований материалов экстремистского и террористического характера, размещённых в сети Интернет.

Перечень вышеперечисленных мер противодействия кибертерроризму не является исчерпывающим и может быть продолжен.

Только комплексная реализация данных мер на федеральном и региональном уровнях позволит существенно снизить уровень кибертеррористических угроз и обеспечить надёжную защищённость критической инфраструктуры.

Литература

1. Владимир Путин обсудил с членами Совета безопасности России меры борьбы с киберугрозами. URL: <https://www.1tv.ru/news/2017-10-26/335153> (дата обращения: 23.02.2018).
2. Голубев В. Электронный терроризм – новое лицо терроризма. //Всемирный антикриминальный антитеррористический форум. 2-я Международная конференция. «Мировое сообщество против глобализации преступности». Изд-во «Экономика», 2004 г. С. 146.

3. *Иванов С.* Кибертерроризм: угроза национальной и международной безопасности. // Информационное агентство оружие России [сайт]. URL: <http://www.arms-expo.ru/news/archive/kiberterrorizm-ugroza-nacional-noy-i-mezhdunarodnoy-bezopasnosti14-03-2013-18-35-00/> (дата обращения: 10.10.2020).
4. *Абдулатипов А. М.* Терроризм в Дагестане. Криминологическое исследование: учеб. пособие. Махачкала: Издательско-полиграфический центр ДГУ, 2002. С. 25.
5. *Турунок С. Г.* Современный терроризм: сущность, причины, модели и механизмы противодействия: учебно-методический комплекс / МГУ им. М. В. Ломоносова; контракт №144/СВ-476 от 04 июля 2008 г. (КНИР «Импульс»), раздел II. М., 2008.
6. Аналитическая справка Антитеррористической комиссии РД: «О состоянии регионального сегмента общегосударственной системы противодействия терроризму в РФ на территории Дагестана в 2018 году».
7. URL: https://www.coe.int/cybercrime_ru (дата обращения 7.05.2020).
8. URL: <https://www.habr.com/post> (дата обращения: 7.05.2020).
9. URL: <https://www.interfax.ru/interview> (дата обращения: 7.05.2020).
10. URL: <https://expert.ru/2017/03/kibervoina> (дата обращения: 7.05.2020).
11. Интервью Председателя Следственного комитета РФ Александра Бастрыкина // Рос. газ. 25 июля. 2017. №162 (7328). С. 4.
12. *Королев А.* Кибертерроризм и информационный терроризм. URL: <http://vpoanalytics.com/2016/02/15/kiberprostranstvo-i-informacionnyj-terrorizm/> (дата обращения: 10.10.2020).
13. Турунок С. Г. Информационный терроризм: выработка стратегии противодействия // Журнал «Общественные науки и современность». 2011. № 4.
14. URL: www.gks.ru/croc/perepis_itogi1612 (дата обращения: 7.05.2020).
15. *Бородин В.Д.* Международный терроризм: генезис, характерные черты и основные тенденции // Наука. Религия. Общество. 2011. № 4.

References

1. Vladimir Putin obsudil s chlenami Soveta bezopasnosti Rossii mery bor'by s kiberugrozami. URL: <https://www.itv.ru/news/2017-10-26/335153> (data obrashcheniya: 23.02.2018).
2. *Golubev V.* Elektronnyi terrorizm – novoe litso terrorizma // Vsemirnyi antikriminal'nyi antiterroristicheskii forum. 2-ya Mezhdunarodnaya konferentsiya. «Mirovye soobshchestvo protiv globalizatsii prestupnosti». Izd-vo «Ekonomika», 2004 g. S. 146.
3. *Ivanov S.* Kiberterrorizm: ugroza natsional'noi i mezhdunarodnoi bezopasnosti // Informatsionnoe agentstvo oruzhie Rossii [sait]. URL: <http://www.arms-expo.ru/news/archive/kiberterrorizm-ugroza-nacional-noy-i-mezhdunarodnoy-bezopasnosti14-03-2013-18-35-00/> (data obrashcheniya: 10.10.2020).
4. *Abdulatipov A. M.* Terrorizm v Dagestane. Kriminologicheskoe issledovanie: ucheb. posobie. Mak-hachkala: Izdatel'sko-poligraficheskii tsentr DGU, 2002. S. 25.
5. *Turonok S. G.* Sovremennyyi terrorizm: sushchnost', prichiny, modeli i mekhanizmy protivodeistviya: uchebno-metodicheskii kompleks / MGU im. M. V. Lomonosova; kontrakt №144/SV-476 ot 04 iyulya 2008 g. (KNIR «Impul's»), razdel II. M., 2008.
6. Analiticheskaya spravka Antiterroristicheskoi komissii RD: «O sostoyanii regional'nogo segmenta obshchegosudarstvennoi sistemy protivodeistviya terrorizmu v RF na territorii Dagestana v 2018 godu».
7. URL: https://www.coe.int/cybercrime_ru (data obrashcheniya 7.05.2020).
8. URL: <https://www.habr.com/post> (data obrashcheniya: 7.05.2020).
9. URL: <https://www.interfax.ru/interview> (data obrashcheniya: 7.05.2020).
10. URL: <https://expert.ru/2017/03/kibervoina> (data obrashcheniya: 7.05.2020).
11. Interv'y u Predsedatelya Sledstvennogo komiteta RF Aleksandra Bastykina // Ros. gaz. 25 iyulya. 2017. №162 (7328). S. 4.
12. *Korolev A.* Kiberterrorizm i informatsionnyi terrorizm. URL: <http://vpoanalytics.com/2016/02/15/kiberprostranstvo-i-informacionnyj-terrorizm/> (data obrashcheniya: 10.10.2020).
13. *Turonok S. G.* Informatsionnyi terrorizm: vyrabotka strategii protivodeistviya // Zhurnal «Obshchestvennye nauki i sovremennost'». 2011. № 4.
14. URL: www.gks.ru/croc/perepis_itogi1612 (data obrashcheniya: 7.05.2020).
15. *Borodin V.D.* Mezhdunarodnyi terrorizm: genezis, kharakternye cherty i osnovnye tendentsii // Nauka. Religiya. Obshchestvo. 2011. № 4.

Поступила в редакцию 25 ноября 2020 г.
Received 25 November, 2020