УДК 351/354

О НЕКОТОРЫХ МЕРАХ ПО СОВЕРШЕНСТВОВАНИЮ ДЕЯТЕЛЬНОСТИ ОРГАНОВ ВНУТРЕННИХ ДЕЛ В ПРОТИВОДЕЙСТВИИ ПРАВОНАРУШЕНИЯМ В ИНФОРМАЦИОННОЙ СФЕРЕ (НА ПРИМЕРЕ РЕСПУБЛИКИ ДАГЕСТАН)
ON SOME MEASURES TO IMPROVE THE ACTIVITIES OF INTERNAL AFFAIRS BODIES IN COUNTERING OFFENSES IN THE INFORMATION SPHERE (ON THE EXAMPLE OF THE REPUBLIC OF DAGESTAN)

Абдулатипов А.М.,
ФГБОУ Дагестанский Государственный Университет, 367000, г. Махачкала, ул. Магомеда Гаджиева, д. 43А.
Abdulatipov A.M.,
Dagestan State University, 367000, Makhachkala, Magomed Gadzhiyev str., 43A.

Аннотация., В статье обосновывается актуальность обеспечения безопасности в информационной сфере в связи с определёнными негативными последствиями глобальной цифровизации в современном мире. В настоящее время ни одно государство не может обходиться без надлежащей информационной безопасности, в поддержке которой ведущая роль принадлежит правоохранительным органам. В исследовании раскрываются некоторые проблемы обеспечения информационной безопасности органами внутренних дел на примере деятельности МВД по РД. Автор отмечает, что недавно созданному для достижения этой цели подразделению МВД по борьбе с киберпреступностью следует по-новому расставить свои акценты в данном направлении не только в информационном, техническом, нормативно-правовом плане, но и в организационном аспекте. В первую очередь, предлагается системная работа по сбору, анализу, обработке и реализации оперативно значимой информации о негативных процессах в информационной сфере и оперативному реагированию на них в пределах своих полномочий. Автор предлагает разработать алгоритм взаимодействия управления по борьбе с киберпреступностью с другими подразделениями МВД и правоохранительными органами, а также специальную программу для подготовки и переподготовки специалистов по борьбе с киберпреступностью. В качестве перспективного направления в рассматриваемой сфере автор предлагает формировать упреждающую модель противодействия информационным правонарушениям.

Annotation. The article substantiates the relevance of ensuring security in the information space in connection with certain negative consequences of global digitalization in the modern world. Currently, no State can exist without proper information security support, in which the leading role belongs to law enforcement agencies. The article reveals some problems of ensuring information security by internal affairs bodies in the context of the activities of the Ministry of Internal Affairs of the Republic of Moldova. The author notes that the newly created department of the Ministry of Internal Affairs for combating cybercrime, which was created to achieve this goal, should put its emphasis in this direction in a new way not only in information, technical, regulatory and legal terms, but also in the organizational aspect. First of all, a systematic work is proposed to collect, analyze, process and implement operationally relevant information about negative processes in the information sphere and, within their authority, promptly respond to them. The author proposes to develop an algorithm for the interaction of the Department for combating cybercrime with other departments of the Ministry of Internal Affairs and law enforcement agencies, as well as a special program for training and retraining specialists in combating cybercrime. As a promising direction in the field under consideration, the author suggests the formation of a proactive model for countering information offenses.

Ключевые слова: органы внутренних дел, информационное пространство, информационная безопасность, защита информации, противодействие информационным угрозам.

Keywords: internal affairs bodies, information space, information security, information protection, countering information threats.

Введение

Проблема обеспечения информационной безопасности, как одной из важнейших элементов национальной безопасности, в настоящее время становится все более актуальной, о чем свидетельствует принятие Президентом Российской Федерации Доктрины информационной безопасности Российской Федерации, утвержденной Указом от 5 декабря 2016 г. №646 [1]. Как указывается в Доктрине, информационная безопасность в Российской Федерации обеспечивается путём защиты информации от фальсификации, повреждения, потери, нарушения целостности данных, их достоверности, доступности и конфиденциальности, а также от несанкционированного доступа неправомочных лиц.

Как отмечается в Стратегии развития информационного общества в Российской Федерации на 2017-2030 годы: «В России информационное общество характеризуется широким распространением и доступностью мобильных устройств (в среднем на одного россиянина приходится два абонентских номера мобильной связи), а также беспроводных технологий, сетей связи. Создана система предоставления государственных и муниципальных услуг в электронной форме, к которой подключились более 34 млн. россиян» [2].

Вместе с тем криминальные структуры не только усваивают такие технологии, но и активно используют их в реализации своих преступных намерений. Наибольшую опасность представляют правонарушения, для совершения которых используются высокие, в том числе компьютерные технологии. Организованные преступные формирования научились активно пользоваться передовыми технологиями в сфере квантовых и облачных технологий, анализа больших чисел, робототехники, искусственного интеллекта, технологии блокчейн, Интернета вещей и т. д.

В настоящее время, как и для всей Российской Федерации, наиболее опасные информационные угрозы Республике Дагестан исходят от деструктивных проектов, курируемых спецслужбами враждебных государств, которые, в основном, используют в качестве прокси-сервера центр информационно – психологических специальных операций (ЦИПСО) СБУ Украины. Высокий уровень опасности этих угроз для нашей страны обусловлен не только внешними, но и внутренними факторами. Об этом свидетельствует и проводимая с 24 мая 2022 года в целях денацификации и демилитаризации Украинской хунты специальная военная операция. Она показала, что некоторая часть граждан Российской Федерации поддерживает нацистскую Украину не только в материальном, финансовом плане, но и осуществлением масштабной информационной войны против своей страны, участием в организации, подготовке и совершении крупных диверсионных и террористических акций на её территории. В качестве примера можно привести подрыв 17 июля 2023 года надводным беспилотником Украины крымского моста, террористический акт 22 марта 2024 года в концертном зале «Крокус Сити Холл» (Красногорск), диверсионно-террористические атаки на мирные жители и объекты гражданской инфраструктуры на приграничной с Украиной территории Российской Федерации. В огромных масштабах распространяется заведомо ложная информация о действиях вооружённых сил и войск национальной гвардии, органов государственной власти Российской Федерации по денацификации и демилитаризации Украины, защите интересов Российской Федерации и ее граждан, поддержанию международного мира и безопасности Такая же информация распространяется и о деятельности добровольческих формирований, организаций и граждан, оказывающих им содействие в выполнении возложенных на них задач.

Сложившая ситуация объективно требует от органов государственной власти и местного самоуправления Российской Федерации принятия адекватны мер, в том числе и по информационному противодействию враждебным силам. Как показывает исследование, в новых условиях необходимо использовать новые подходы противостояния информационным угрозам. Всё это в равной мере относится и к правоохранительным органам, в том числе и органам внутренних дел.

В связи с этим, **объектом исследования** данной научной работы выбрано изучение опыта работы органов и подразделений МВД по Республике Дагестан по противодействию угрозам информационной безопасности.

В качестве **методов исследования** использованы изучение нормативных и аналитических документов МВД по РД, анализ различных направлений деятельности органов и подразделений внутренних дел в борьбе с правонарушениями в информационной сфере, а также сравнительный анализ статистических данных о таких правонарушениях.

Как отмечает Л. Л. Грищенко и другие учёные: «Достаточно популярной с началом специальной военной операции на Донбассе в средствах массовой информации не только Украины, но и стран Запада стала технология «держи вора». Чувствуя провалы в своих действиях, руководство киевского режима первыми поднимает крик о якобы имеющих место «зверствах российской армии» и направляет гнев своего народа в сторону России» [3, с.132]. Для этого ими используются различные так называемые «грязные» информационные технологии и провокации

В частности, к проектам информационной войны против Республики Дагестан можно отнести постоянно возобновляемые ими телеграм-каналы «Утро Дагестан», 1adat и другие. К реализации этих проектов привлекаются также разыскиваемые в России за измену родине Илья Пономарев, за террористическую деятельность - Абу Умар Саситлинский, Абдулла Костекский и другие. Их админы находятся в Киеве, Турции и других странах.

При этом, для дестабилизации обстановки спецслужбами враждебных государств активно используются имеющиеся и возникшие в республике проблемные ситуации. Так, после обращения Президента РФ о мобилизации, с 21 сентября 2022 года деструктивные элементы стали распространять в социальных сетях заведомо ложную информацию о мобилизации 13 тысяч жителей Дагестана для участия в СВО и необходимости проведения анти мобилизационных митингов и протестных акций. После чего, 25 сентября жителями селения Эндирей Хасавюртовского района была организована массовая протестная акция с блокировкой автодороги Хасавюрт – Махачкала, которая сопровождалась стычками протестующих лиц с правоохранителями. Такие же, но менее масштабные противоправные акции происходили в городах Махачкала, Хасавюрт, Дербент и селении Бабаюрт. Также были случаи подготовки противоправных действий против военных комиссариатов республики и их сотрудников.

Также был использован палестино-израильский конфликт для распространения в информационном пространстве республики призывов организовать массовые протестные акции. Так, 28 октября 2023 г. в г. Хасавюрте возле гостиницы «Фламинго» собралось до 400 человек с требованиями выселить из гостиницы якобы проживающих там лиц еврейской национальности, хотя их там вообще не было.

29 октября 2023 г. на территории международного аэропорта «Уйташ» г. Махачкалы под предлогом выражения солидарности с народом Палестины и недопущения на территорию республики граждан Израиля, группой лиц в количестве до 1500 человек был проведён несанкционированный митинг. В результате провокационных действий подстрекателей митинг перерос в массовые беспорядки, в том числе с проникновением на территорию охраняемого объекта и противодействия законным требованиям правоохранительных органов, нанесением ущерба инфраструктуре международного аэропорта.

Также, в августе 2023 г. с подачи администраторов канала «Утро Дагестан» были организованы перекрытия автодорог в г. Махачкале в связи с массовыми отключениями энергоснабжения.

Особую опасность представляют попытки вовлечения международными террористическими организациями и украинскими спецслужбами через мессенджеры подростков и молодёжь республики в диверсионно-террористическую деятельность. По данным Центра противодействия экстремизму МВД по РД[4], 4 января 2024 г. уроженец РД А. (несовершеннолетний), скрытно проникнув на взлетно-посадочную полосу, расположенную на территории в/ч № 86789 в г. Челябинске, совершил поджог воздухозаборника истребителя-бомбардировщика СУ-34 Вооружённых Сил РФ. Также установлена его причастность к поджогам 27 ноября 2023 г. релейного шкафа «41-43 ШГУ-М» на станции № 6 железнодорожной пути «Шамхал-Буйнакск» и 3 декабря 2023 г. в г. Буйнакске металлической будки с оборудованием сотовой связи ПАО «Вымпелком» («Билайн»). При осмотре его сотового телефона обнаружена переписка с куратором Украинских спецслужб, который завербовал его через социальные сети в интернет-мессенджере «Телеграм» и обещал за поджоги на объектах жизнеобеспечения, транспортной и военной инфраструктуры денежные вознаграждения.

Ведущая роль в обеспечении безопасности в информационном пространстве принадлежит правоохранительным органам, в том числе и органам внутренних дел. Законодательством Российской Федерации на МВД России и его территориальные органы возложены задачи по обеспечению общественной безопасности, охране общественного порядка, анализу и прогнозу миграционных процессов и борьбе с преступностью. Как показывает правоприменительная практика, в современный период информация нередко становится катализатором различного рода противоправных акций против общественной безопасности и общественного порядка, которые сопровождаются масштабными общественно опасными последствиями и широким общественным резонансом.

Как отмечает В.А. Кемпф: «В настоящее время МВД РФ вопросы развития и внедрения автоматизированных информационных систем в деятельности органов внутренних дел, в т.ч. применения передовых подходов и технологий информатизации МВД России, стоят на одном из первых мест» [5, с. 25].

В целях противодействия распространению в информационном пространстве через различные мессенджеры идеологии экстремизма, терроризма, криминальной субкультуры, подразделениями МВД по РД осуществляется комплекс оперативно-профилактических, оперативно – розыскных, административно-режимных и профилактических мер. На постоянной основе проводится мониторинг наиболее популярных в регионе Интернет-ресурсов на предмет выявления фактов размещения противоправного контента, призывов к деструктивных деятельности, к протестным акциям.

Исследование показывает, что наиболее эффективными в противодействии распространению заведомо ложной информации о социально-значимых процессах в республике, разоблачению деструктивной деятельности отдельных граждан и групп лиц (интернет-сообществ) являются пропагандистские и контр пропагандистские мероприятия в региональном сегменте сети Интернет, в том числе путем создания и продвижения антитеррористического контента.

По данным ИЦ МВД по РД [6], в 2023 г. в ходе указанных выше мероприятий выявлено 26 (54; -61,1%) преступлений (по ст. 205. 2 УК РФ – 9, ст. 280 УК РФ – 12, ст. 207.3 УК РФ – 5) а также 308 (293; +5,1%) административных правонарушений (по ст. 20.1 ч.3– 4, ст. 20.2 ч.1– 19, ст. 20.3– 234, ст. 20.3.1–14, ст. 20.3.2– 2, ст. 20.3.3 ч.1– 16, ст. 20.29– 17, ст. 13.15 ч.9 КоАП РФ – 1). Для блокирования доступа к Интернет-ресурсам, признанным решениями судов РФ экстремистскими и внесёнными в федеральный список экстремистских материалов (сайт Министерства Юстиции России «minjust.ru») в Управление Роскомнадзора по РД направлена 4051 ссылка на неправомерный контент в сети Интернет. Все они внесены в «Единый реестр доменных имен, указателей страниц сайтов в сети Интернет и сетевых адресов,

позволяющих идентифицировать сайты, содержащие информацию, распространение которой в РФ запрещено». Также выявлено и направлено в прокуратуру для организации блокирования доступа 107 Интернет-ресурсов, размещённых на зарубежных доменах, с информацией о призывах к участию в массовых протестных акциях, либо в иных противоправных действиях.

Также были предприняты меры по борьбе с попытками дестабилизации обстановки путем многочисленных анонимных заведомо ложных сообщений об актах терроризма. Если в 2022 г. их было зарегистрировано 123, то в январе-декабре 2023 г. удалось снизить до 83 случаев (-32,5%).

Органы внутренних дел республики в своей деятельности в данном направлении опираются не только на помощь специальных сил и средств, но и на помощь общественности и граждан, особенно волонтёрских движений.

Как справедливо отмечает А. Л. Осипенко: «При этом возможно расширение правоохранительной деятельности в киберпространстве за счет привлечения сетевой общественности. Полагаем, полиция должна принимать участие в формировании норм сетевого поведения и традиций уважения к нормам права со стороны пользователей сети, совершенствовании форм взаимодействия органов внутренних дел и гражданского общества через интернет-ресурсы. Кроме того, особые группы активных пользователей под контролем представителей органов внутренних дел вполне могут быть задействованы в поддержании правопорядка и обеспечении интересов общества в кибер-пространстве» [7, с. 40].

Как показывает исследование, о высокой превентивной эффективности такого взаимодействия свидетельствуют результаты совместной с другими ведомствами, общественными формированиями и религиозными объединениями работа в образовательных организациях по повышению уровня правосознания и правовой культуры учащихся и студентов. Только в прошлом году подразделениями МВД по РД проведено 60 таких мероприятий, в ходе которых слушателям разъясняются правовые положения об уголовной и административной ответственности за распространение в социальных сетях материалов с экстремистским содержанием, пропаганду идей запрещенных на территории РФ международных террористических организаций, за организацию и участие в несанкционированных протестных акциях, а также даются рекомендации, как вести себя в случае попытки вербовки в террористические и экстремистские структуры через мессенджеры.

За последние годы органы внутренних дел республики столкнулись с проблемой распространения преступных посягательств, которые совершаются в целях генерации (майнинга) криптовалюты. Генерация криптовалюты сопровождается также с масштабным хищением электроэнергии.

Так, по данным МВД по РД, в 2022 году совместно с сотрудниками ФСБ выявлена сеть из 17 майнинг-ферм. Организованная преступная группа подпольно добывала криптовалюту в городах и отдалённых сельских населённых пунктах республики. О масштабах преступной деятельности майнеров можно судит только по изъятой у них компьютерной техники, видеокарт на общую сумму более чем 500 миллионов рублей.

По информации компании "Россети", в последнее время Дагестан занимает первое место среди регионов СКФО по числу незаконных майнинг-ферм. За прошлый год специалисты энергопредприятия совместно с правоохранительными органами выявили в республике 25 случаев кражи электроэнергии, которую использовали для добычи криптовалюты на общую сумму 130 миллионов рублей. Майнеры похитили электричества на 50 миллионов киловатт-часов, что сопоставимо с годовой выработкой Гунибской ГЭС в горах Дагестана [9].

Для противодействия незаконному майнинг- бизнесу и изъятию у преступных групп незаконных майнинг-устройств по инициативе МВД по РД была создана межведомственная

комиссия, которая проводила рейды, подворные обходы и прочёсывание местности в отдельных населённых пунктах республики. По данным МВД, только в Левашинском районе обнаружено и ликвидировано 17 незаконных ферм по добыче криптовалюты.

Как известно, различные подразделения МВД имеют строго очерченные свои полномочия. Так, подразделения охраны общественного порядка реализуют свои функции, в основном, путём профилактики правонарушений (подворные, поквартирные обходы, профилактический учет, адресные мероприятия и т. д.), а подразделения уголовного розыска, специальных технических мероприятий (Управление «К») осуществляют свои полномочия по борьбе с конкретными преступлениями. Подразделения по противодействию экстремизму имеют опыт оперативно-розыскной, административно-правовой и профилактической работы по противодействию информационным правонарушениям экстремистского и террористического характера. Однако, информационные правонарушения охватывают и другие сферы, к примеру, распространение через мессенджеры криминальной субкультуры, мошенничества в сфере цифровых технологий и электронных средств платежей, создание суицидальных сообществ («групп смерти»), правонарушения в сфере оборота электронных денег (криптовалют), «Колумбайн» и «Скулшутинг», «Фишинг» и т. д. В связи с этим, Указом Президента РФ [8] в структуре МВД создано новое оперативное подразделение по организации борьбы с противоправным использованием информационно-коммуникационных технологий (киберпреступностью), которое осуществляет также мониторинг сетевых ресурсов и профилактику в цифровой среде. В настоящее время идёт процесс формирования данной структуры.

Таким образом, органы и подразделения внутренних дел непосредственно принимают активное участие в решении важнейших задач по обеспечению информационной безопасности страны, совершенствованию системы противодействия информационным правонарушениям, обеспечению активного взаимодействия и координации работы всех задействованных структур. Вместе с тем, в этой деятельности имеются много проблем, решению которых руководством нашей страны и её субъектов уделяется серьёзное внимание.

Выводы

Подводя итоги, необходимо отметить, что в настоящее время новому подразделению МВД по борьбе с киберпреступностью следует выстроить свою деятельность не только в информационном, техническом, нормативно-правовом плане, но и в организационном аспекте. Основные усилия, по мнению многих учёных, следует направить на формирование упреждающей модели противодействия информационным правонарушениям. Суть такой модели заключается в своевременном получении упреждающей информации о признаках подготовки неправомерных действий в информационной сфере, выявлении, предупреждении и пресечении киберпреступлений и других правонарушений в информационной сфере на стадии приготовления и покушения на их совершение. Считаю, что такая модель должна опираться на наиболее эффективных методах информационного противодействия опасным криминальным проявлениям, одним из которых является мониторинг подозрительных закрытых форумов. Как показало исследование опыта МВД по РД, с его помощью органы внутренних дел устанавливают и своевременно пресекают покушения на потенциальные жертвы киберпреступлений, тем самым повышая уровень безопасности объектов правовой охраны в данной сфере. Такая модель позволяет также эффективно противодействовать деструктивному влиянию криминалитета на подростков и молодёжь, пресечению попыток вовлечения их в преступные структуры

Представляется, что системная работа по сбору, анализу и обработке и реализации оперативно значимой информации о негативных процессах в информационном пространстве и

оперативному реагированию в пределах своих полномочий позволит значительно снизить уровень информационных преступлений и административных правонарушений.

Следует отметить также важность разработки алгоритма взаимодействия управления по борьбе с киберпреступностью с подразделениями МВД и другими правоохранительными органами в сфере своих полномочий, а также изучение для внедрения в своей практической деятельности накопленного ими опыта в противодействии отдельным преступлениям, совершаемым с использованием сетевых ресурсов и мессенджеров.

Необходимо разработать также программу подготовки и переподготовки специалистов в сфере противодействия информационным правонарушениям. Как справедливо отмечает А. Л. Осипенко, необходимо «качественное повышение уровня подготовки российских специалистов по противодействию киберпреступности за счет активного внедрения практико- ориентированных подходов, использования передового зарубежного и российского опыта» [7, с. 41].

Важное значение для осуществления функции сетевого мониторинга имеет создание правовых оснований для доступа сотрудников подразделения по борьбе с киберпреступностью к информационным ресурсам различных государственных органов, коммерческих и иных структур, провайдеров и операторов интернет - связи, а также представителей Mesh-сети, использующих для соединения абонентов между собой в социальных сетях и мессенджерах посредством радиочастотной связи через Wi-Fi-маршрутизаторы.

В заключении необходимо отметить, что проблем в деятельности органов внутренних дел по обеспечению информационной безопасности очень много и, естественно, на их решение уйдёт определённое время. Важно, чтобы не экономить на этом сил и средств, так как упущения могут привести к необратимым последствиям и расходу кратных средств на устранение этих последствий.

Список использованных источников

1. «Об утверждении Доктрины информационной безопасности Российской Федерации»: Указ Президента Российской Федерации от 5 декабря 2016 г. №646 //СПС «Консультант плюс». – Режим доступа: https://www.consultant.ru/ law/hotdocs/48076.html (Дата обращения: 25.04.2024)

2. О Стратегии развития информационного общества в Российской Федерации на 2017-2030 годы: Указ Президента РФ от 9 мая 2017 г. № 203. /СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_216363/ (Дата обращения: 25.04.2024)

3. Грищенко Л. Л., Синодов И. А. Роль и место МВД России в обеспечении информационной безопасности. [Электронный документ]/Сетевое издание «Академическая мысль». - № 4. – 2022. – с. 130 – 135. - Сайт: https://а.мвд.рф/ nauka /-академическая-мысль-/архив-номеров (Дата обращения: 25.04.2024)

4. Аналитическая справка ЦПЭ МВД по РД о состоянии оперативной обстановки и результатах работы в сфере противодействия экстремизму и терроризму за 12 месяцев 2023 года

5. Кемпф, В.А. Обеспечение информационной безопасности в ОВД: учебное пособие. – Барнаул: Барнаульский юридический институт МВД России, 2019. – 63 с.

6. Статистические таблицы ИЦ МВД по РД

7. Осипенко, А. Л. Об участии органов внутренних дел в системе обеспечения кибербезопасности Российской Федерации // «Общество и право». – 2018. - № 3 (65). – С. 35 - 43

8. Указ Президента Российской Федерации от 30 сентября 2022 г. № 688 «О внесении изменений в некоторые акты Президента Российской Федерации» //СПС «Консультант плюс». – Режим доступа: https://www. consultant.ru/document/cons_doc_LAW_4 27884/ (Дата обращения: 20.02.2024).

9. «Россети Северный Кавказ» за полгода выявили в Дагестане майнинг-хищения электроэнергии на 23 млн рублей. - [Электронный ресурс] /Официальный сайт «Россети Северный Кавказ». – Ссылка: https://www.rossetisk.ru/press_center/company_news/ rosseti-severnyy-kavkaz-za-polgoda-vyyavili-v-dagestane-mayning-khishcheniya-elektroenergii-na-23-ml/ (Дата обращения: 27.04.2024)