

Дата поступления рукописи в редакцию: 04.07.2026 г.
Дата принятия рукописи в печать: 27.07.2026 г.

DOI: 10.24412/2076-1503-2026-8-834-836

ФОМИЧЕВ Денис Сергеевич,
преподаватель кафедры огневой подготовки
Санкт-Петербургского университета МВД России,
e-mail: dan_fds@inbox.ru

К ВОПРОСУ О ПРОТИВОДЕЙСТВИИ РАСПРОСТРАНЕНИЮ ЭКСТРЕМИСТКОЙ ИДЕОЛОГИИ В СЕТИ ИНТЕРНЕТ: МЕТОДЫ И ТЕХНОЛОГИИ В ПРОФИЛАКТИКЕ ПРОТИВОДЕЙСТВИЯ

Аннотация. Автор в своей научной статье проводит анализ способов использования возможностей сети Интернет экстремистскими организациями, а также методов и технологий противодействия проявлениям экстремизма в сети Интернет.

Ключевые слова: профилактика, противодействие, государство, власть, правоохранительные органы, информация, экстремизм, преступление, технологии, безопасность, законодательство.

FOMICHEV Denis Sergeevich,
Lecturer, Department of Firearms Training St. Petersburg University
of the Ministry of Internal Affairs of Russia

ON THE ISSUE OF COUNTERING THE SPREAD OF EXTREMIST IDEOLOGY ON THE INTERNET: METHODS AND TECHNOLOGIES IN THE PREVENTION OF COUNTERACTION

Annotation. In his scientific article, the author analyzes the ways in which extremist organizations use the Internet, as well as methods and technologies to counter extremism on the Internet.

Key words: prevention, counteraction, state, government, law enforcement agencies, information, extremism, crime, technology, security, legislation.

Основная проблема противодействия экстремизму в сети Интернет во многом объясняется наличием у преступных сообществ значительного научно-технического потенциала, поскольку они привлекают в свои ряды целые группы квалифицированных специалистов в области высоких технологий.

Следует отметить, что процедура внесения сайтов в единый реестр Интернет-ресурсов, запрещенных законом довольно трудоёмкая и не всегда эффективная. Дело в том, что в соответствии с ФЗ № 149 от 27.07.2006 «Об информации, информационных технологиях и о защите информации», для того чтобы внести определенный сайт в реестр запрещенных законом Интернет-ресурсов, необходимо пройти определенный перечень процедур, который может продлиться несколько суток. К сожалению, довольно часто, этого времени бывает достаточно, чтобы данный Интернет-ресурс выполнил свои задачи.

В настоящее время в области противодей-

ствия экстремизму и терроризму в глобальном информационном пространстве актуальными и проблемными являются следующие вопросы технического плана:

идентификация личности, разместившей материалы экстремистского или террористического характера;

идентификация пользователя как автора материала террористической или экстремистской направленности, а не как владельца средств вычислительной техники, с помощью которых в глобальной сети был размещен данный материал.

Эффективными способами защиты социальных сетей от несанкционированного доступа целесообразно считать следующие:

1. Верификация всех страниц социальной сети.
2. Штрафование пользователей социальных сетей за призывы к экстремистским действиям.
3. Запрет на пользование социальными сетями определённых категорий осуждённых.

Следует отметить, что значительная часть Интернет-ресурсов несмотря на то, что ориентированы сугубо на российских пользователей, физически и юридически расположены за пределами Российской Федерации, и эта одна из проблем в области технического противодействия экстремизму и терроризму в информационном пространстве. Данная ситуация также осложняется и тем, что экстремисты, как правило, используют хостинги ряда государств, которые не отличаются позитивным отношением к России.

Актуальным является вопрос о специализированной подготовке сотрудников подразделений системы МВД, осуществляющих деятельность по противодействию информационному экстремизму. Исследователями в данном направлении отмечается отсутствие надлежащей квалификации сотрудников ОВД, ведущих борьбу с экстремистскими проявлениями в киберпространстве и необходимости расширения их технических возможностей. Для повышения эффективности подготовки квалифицированных кадров в области противодействия экстремизму и терроризму в соответствии с Приказом МВД России от 29.08.2012 № 820 за Краснодарским университетом МВД России и ВИПК МВД России был закреплён профиль подготовки сотрудников ОВД РФ «Деятельность подразделений по противодействию экстремизму, терроризму и борьбе с организованной преступностью». В данных образовательных организациях осуществляется подготовка квалифицированных кадров для подразделений по противодействию экстремизму и терроризму. Разработка программ обучения по данному направлению осуществляется во взаимосвязи с ГУПЭ МВД России, ГУОООП МВД России, ГУУР МВД России.

Органы государственной власти уделяют большое внимание проблемам обеспечения технического противодействия экстремизму в сети Интернет. Об этом говорят вносимые поправки в законодательные акты РФ. В целях повышения эффективности работы подразделений системы МВД России по противодействию экстремизму, образовательными организациями МВД России проводится подготовка квалифицированных кадров в данной области. Однако, с учетом особенностей экстремизма и терроризма в глобальном информационном пространстве возникает ряд юридических и технических проблем, связанных с доработкой нормативно-правовой базы в данной области, введением процесса всеобщей персонификации, организации надежной системы сотрудничества и взаимодействия с правоохранительными органами зарубежных стран.

Кроме того одним из важных направлений работы по защите информационного пространства

от преступной деятельности экстремистских организаций является противодействие хакерам, которые привлекаются экстремистами для совершения атак на автоматизированные системы управления государствами и информационно-телекоммуникационные сети.

Вопросы защиты информации в Российской Федерации возложены на Федеральную службу по техническому и экспортному контролю (ФСТЭК), которая сменила Гостехкомиссию РФ. Требования, которые были разработаны ФСТЭК еще в 2010-х годах, являлись обязательными к исполнению, но, по мнению специалистов, предельно техническими и мало учитывающими управленческие и организационные вопросы при обеспечении информационной безопасности.

В соответствии с указом Президента РФ от 22 декабря 2017 года № 620, функции предупреждения, обнаружения и ликвидации последствий компьютерных атак возложены на Федеральную службу безопасности Российской Федерации.

Условно системы информационной безопасности можно разделить на две категории:

- системы предотвращения угроз (управления доступом);
- системы мониторинга активности.

Проблема противодействия хакерским атакам, в частности, направленным на дестабилизацию критически важных информационных систем РФ, сегодня является одной из первоочередных задач органов государственной власти. Актуальность проблемы подтверждает рост количества кибератак на системы управления критически важными инфраструктурами государства, включая военную сферу, ядерную и топливную энергетику, системы опасных производств, что может повлечь за собой дестабилизацию государства, огромные материальные потери, экологические катастрофы, глобальные жертвы и разрушения.

Угроза кибертерроризма сегодня остаётся весьма актуальной, а ее эффективное преодоление возможно только совместными усилиями всех стран с развитой информационной инфраструктурой на основе принципов планомерности и системного подхода.

Вместе с тем, основными мерами информационного противодействия следуют считать информационно-пропагандистские меры, которые направлены на выявление сущности и организацию разъяснительной работы об опасности различных проявлений экстремизма и терроризма, осуществлению воздействия на сознание граждан в целях формирования неприятия идеологии насилия, жестокости и привлечения их к участию в противодействии экстремизму и терроризму.

В виду чего, на современном этапе, одной из

наиболее важных задач органов государственной власти является активизация противодействия распространению идеологии экстремизма и терроризма и организация информационно-пропагандистского обеспечения в целях осуществления антиэкстремистских и антитеррористических мероприятий в едином мировом информационном пространстве.

В рамках реализации основных направлений государственной политики в сфере противодействия экстремизму и терроризму, следует отметить положительный опыт проведения Интернет-семинаров в целях обсуждения актуальных проблем противодействия идеологии экстремизма и терроризма с использованием возможностей глобального информационного пространства. Возможности для увеличения масштабов аудитории при этом практически безграничны и определяются предварительным информированием потенциальных участников Интернет-семинаров.

Таким образом, можно отметить, что только совместная конструктивная деятельность органов государственной власти, образовательных, научных, общественных и религиозных организаций в общем, а также каждого сознательного гражданина в отдельности, способна результативно противодействовать распространению экстремистских взглядов и террористических идей в глобальной сети Интернет.

Список литературы:

[1] Единый федеральный список организаций, в том числе иностранных и международных организаций, признанных в соответствии с законодательством Российской Федерации террористическими. // Федеральная Служба Безопасности. URL: <http://www.fsb.ru/fsb/npd/terror.htm> (дата обращения: 12.05.2024).

[2] Перечень общественных объединений и религиозных организаций, в отношении которых судом принято вступившее в законную силу решение о ликвидации или запрете деятельности по основаниям, предусмотренным Федеральным законом от 25.07.2002 № 114-ФЗ «О противодействии экстремистской деятельности». // Минюст РФ. URL: <https://minjust.gov.ru/ru/documents/7822/> (дата обращения: 12.05.2024).

[3] Вся статистика интернета и социальных сетей на 2023 год — цифры и тренды в мире и в России. // Digital-агент-

ство WebCanape. URL: <https://www.web-canape.ru/business/vsya-statistika-interneta-i-socsetej-na-2023-god-cifry-i-trendy-v-mire-i-v-rossii/>. (дата обращения: 12.05.2023).

[4] Экстремизм представлен в основном возрастной группой. Молодежный экстремизм как одна из наиболее актуальных социально – политических проблем в России. // Not-Not. URL: <https://not-not.ru/eda/ekstremizm-predstavlen-v-osnovnom-vozhrazstnoigruppoi.html> (дата обращения: 12.05.2024).

[5] Стратегия противодействия экстремизму в Российской Федерации до 2025 года (утв. Президентом РФ от 28 нояб. 2014г. № Пр-2753) // Совет Безопасности Российской Федерации. URL: <http://www.scrf.gov.ru> (дата обращения: 12.05.2024).

References:

[1] Unified federal list of organizations, including foreign and international organizations, recognized as terrorist in accordance with the legislation of the Russian Federation. // Federal Security Service. URL: <http://www.fsb.ru/fsb/npd/terror.htm> (date accessed: 12.05.2024).

[2] List of public associations and religious organizations in respect of which a court has made a final decision to liquidate or prohibit their activities on the grounds stipulated by Federal Law No. 114-FZ of 25.07.2002 "On Counteracting Extremist Activity". // Ministry of Justice of the Russian Federation. URL: <https://minjust.gov.ru/ru/documents/7822/> (date accessed: 12.05.2024).

[3] All internet and social media statistics for 2023 - figures and trends worldwide and in Russia. // Digital agency WebCanape. URL: <https://www.web-canape.ru/business/vsya-statistika-interneta-i-socsetej-na-2023-god-cifry-i-trendy-v-mire-i-v-rossii/>. (Accessed: 12.05.2023).

[4] Extremism is represented mainly by an age group. Youth extremism as one of the most pressing socio-political problems in Russia. // Not-Not. URL: <https://not-not.ru/eda/ekstremizm-predstavlen-v-osnovnom-vozhrazstnoigruppoi.html> (Accessed: 12.05.2024).

[5] Strategy for countering extremism in the Russian Federation until 2025 (approved by the President of the Russian Federation on November 28, 2014, No. Pr-2753) // Security Council of the Russian Federation. URL: <http://www.scrf.gov.ru> (date accessed: 12.05.2024).

