

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ

**Организация работы в сфере противодействия распространению
экстремистской, террористической и иной деструктивной
информации в сети «Интернет»**

Прокуратура
Ханты-Мансийского
автономного округа - Югры

Управление национальной политики
Департамента внутренней политики
Ханты-Мансийского
автономного округа – Югры

Ханты-Мансийск, 2026 год

ОГЛАВЛЕНИЕ

1. ВВЕДЕНИЕ	2
2. ОСНОВНЫЕ ПОНЯТИЯ И ЗАКОНОДАТЕЛЬНЫЕ ОСНОВЫ	2
3. ОРГАНИЗАЦИЯ РАБОТЫ В АДМИНИСТРАЦИИ МУНИЦИПАЛЬНОГО ОБРАЗОВАНИЯ	3
4. ПОРЯДОК ДЕЙСТВИЙ ПРИ ВЫЯВЛЕНИИ ЗАПРЕЩЕННОЙ ИНФОРМАЦИИ	4
5. КОНТРОЛЬ ЗА ПОДВЕДОМСТВЕННЫМИ УЧРЕЖДЕНИЯМИ	5
6. РЕКОМЕНДАЦИИ	6
7. ИТОГИ	6

1. ВВЕДЕНИЕ

В современном мире сеть «Интернет» является не только источником полезной информации, но и средой для распространения противоправного контента: экстремистских, террористических материалов, фейков, призывов к незаконным действиям. Это создает прямые угрозы безопасности граждан и общественному порядку.

Ханты-Мансийский автономный округ – Югра является одним из лидеров по уровню интернет-проникновения (более 91% населения имеют доступ к сети). Указанный факт (при определенных условиях) может использоваться для радикализации населения. Это накладывает на органы местного самоуправления особую ответственность за информационную безопасность.

Органы местного самоуправления (далее - ОМСУ) являются важными субъектами в системе противодействия экстремизму и терроризму. Их задача - не просто реагировать на уже выявленные нарушения, но и вести системную профилактическую работу, а также оперативно информировать уполномоченные органы (в первую очередь территориальный отдел прокуратуры и Роскомнадзор) о выявленных фактах распространения запрещенной информации.

2. ОСНОВНЫЕ ПОНЯТИЯ И ЗАКОНОДАТЕЛЬНЫЕ ОСНОВЫ

До начала работы необходимо понимать и усвоить какая информация подлежит блокировке, а также знать перечень нормативных актов, регулирующих эту сферу.

Что подлежит ограничению/блокировке?

1. Экстремистские материалы: Информация, включенная в Федеральный список экстремистских материалов (ведется Минюстом России <https://minjust.gov.ru/ru/extremist-materials/>). Тексты, аудио-, видеозаписи, изображения, признанные судом экстремистскими.

2. Информация, запрещенная для распространения (ст. 15.3 Федерального закона Российской Федерации от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации») включая:

- призывы к массовым беспорядкам, экстремизму, участию в несанкционированных митингах;
- заведомо ложные сообщения об актах терроризма и недостоверная общественно значимая информация (фейки);

- информация, дискредитирующая Вооруженные Силы Российской Федерации, а также призывы к воспрепятствованию их деятельности;
- призывы к введению санкций против Российской Федерации;
- обоснование и оправдание экстремизма и терроризма;
- материалы иностранных организаций, признанных нежелательными или запрещенными на территории Российской Федерации.

3. Информация о способах изготовления оружия, взрывчатых веществ, боеприпасов.

Основные нормативные документы, на которые следует опираться в работе:

Федеральный закон Российской Федерации от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

Федеральный закон Российской Федерации от 25.07.2002 № 114-ФЗ «О противодействии экстремистской деятельности»;

Федеральный закон Российской Федерации от 06.03.2006 № 35-ФЗ «О противодействии терроризму»;

Стратегия национальной безопасности Российской Федерации (Указ Президента Российской Федерации от 02.07.2021 № 400);

Стратегия противодействия экстремизму в Российской Федерации (Указ Президента Российской Федерации от 28.12.2024 № 1124).

Постановление Правительства РФ от 26.10.2012 № 1101 «О единой автоматизированной информационной системе «Единый реестр доменных имен, указателей страниц сайтов в информационно-телекоммуникационной сети «Интернет» и сетевых адресов, позволяющих идентифицировать сайты в информационно-телекоммуникационной сети «Интернет», содержащие информацию, распространение которой в Российской Федерации запрещено».

3. ОРГАНИЗАЦИЯ РАБОТЫ В АДМИНИСТРАЦИИ МУНИЦИПАЛЬНОГО ОБРАЗОВАНИЯ

Для эффективной и результативной реализации данного направления необходимо организовать эту работу внутри муниципалитета на системной основе.

Первоочередные шаги:

1. Назначить ответственное лицо (лиц), которое будет заниматься мониторингом сети «Интернет» и взаимодействием с надзорными органами. Закрепить его обязанности в должностной инструкции

(регламенте).

2. Обеспечить ответственное лицо рабочим местом с бесперебойным и расширенным доступом в сеть «Интернет» и необходимым программным обеспечением для создания скриншотов (снимков экрана).

3. Включить в муниципальную программу мероприятия по мониторингу интернет-пространства и информационном противодействии экстремизму и терроризму.

4. Организовать взаимодействие с подведомственными учреждениями (школы, библиотеки, клубы, спортивные центры). Дать указание и обеспечить включение в их обязанности сверку печатной и аудиовизуальной продукции с Федеральным списком экстремистских материалов.

5. Активно участвовать в работе муниципальных антитеррористических комиссий и комиссий по противодействию экстремизму. Регулярно выносить на их заседания вопросы, связанные с профилактикой распространения деструктивной информации.

4. ПОРЯДОК ДЕЙСТВИЙ ПРИ ВЫЯВЛЕНИИ ЗАПРЕЩЕННОЙ ИНФОРМАЦИИ

Если в ходе мониторинга обнаружен подозрительный контент, необходимо следовать следующему алгоритму:

Шаг 1. Проверка и фиксация.

1. Идентификация информации.

Определение, к какой категории она относится (экстремистский материал, призыв, фейк и т.д.).

2. Проверка наличия в реестрах:

- в Федеральном списке экстремистских материалов на сайте Минюста России: <http://minjust.ru/ru/extremist-materials>.

- в Едином реестре запрещенной информации Роскомнадзора: <http://eais.rkn.gov.ru/> (проверка, не заблокирован ли уже ресурс). Если адреса в реестре нет, блокировка еще не осуществлена.

3. Фиксация скриншота (снимок экрана).

Зафиксировать страницу целиком, чтобы было видно текст, видео, автора публикации, URL-адрес и дату. Скриншоты - главное доказательство для направления обращения.

Шаг 2. Куда и как обращаться.

В зависимости от вида выявленной информации, необходимо направить информацию в разные инстанции.

а) Если информация содержится в Федеральном списке экстремистских материалов:

Куда направлять: В прокуратуру (в территориальный отдел или прокуратуру округа), в территориальные органы внутренних дел (МВД России).

Что направить: Обращение, в котором указать URL-адрес страницы, реквизиты судебного решения о признании материала экстремистским и его номер по списку Минюста. Приложить скриншоты.

б) Если информация подпадает под ст. 15.3 ФЗ-149 (призывы, фейки, дискредитация ВС РФ и т.д.):

Куда направлять: В прокуратуру (в территориальный отдел или прокуратуру округа). У муниципалитетов нет прямых полномочий требовать блокировки таких материалов в Роскомнадзор - это полномочие прокуратуры.

Что направить: Сопроводительное письмо с описанием ситуации, скриншотами и обоснованием, почему эта информация, по вашему мнению, подлежит блокировке. Прокуратура проверит эти материалы и, в случае обоснованности, направит требование о блокировке в Роскомнадзор.

в) Если информация содержит сведения об изготовлении оружия или взрывчатки:

Куда направлять: В территориальные органы внутренних дел (МВД России). Эта процедура также осуществляется по каналам МВД.

Что направлять: Обращение, в котором указать URL-адрес страницы. Приложить скриншоты.

5. КОНТРОЛЬ ЗА ПОДВЕДОМСТВЕННЫМИ УЧРЕЖДЕНИЯМИ

Не только выявление угроз в интернете, но и контроль за деятельностью учреждений (школ, больниц, домов культуры спорта).

При проверках обращается внимание на:

1. Наличие локальных актов.

Приказы, инструкции, обязывающие сотрудников проводить сверку литературы (в библиотеках, учебных фондах) с Федеральным списком экстремистских материалов.

2. Доступ к интернету.

Осуществление фильтрации контента на компьютерах в общедоступных местах (библиотеки, классы). Использование системы контент-фильтрации для исключения доступа к запрещенным сайтам (Это

касается и публичного Wi-Fi).

3. Профилактическая работа.

Проведение в учреждениях мероприятий, направленных на формирование у молодежи нетерпимости к экстремистской идеологии, медиаграмотности (умение отличать фейки).

6. РЕКОМЕНДАЦИИ

Системность.

Работа по мониторингу осуществляется регулярно. Это направление включается в планы работы на месяц/квартал.

Взаимодействие.

Тесное взаимодействие с территориальным прокурором. Оперативное (в течение суток) направление информации по всем сомнительным случаям. Это ключевая точка опоры для внесудебной блокировки.

Ответственность.

За непринятие мер может последовать представление прокурора, а в случае выявления фактов распространения экстремистских материалов в подведомственных учреждениях - и более серьезные последствия.

Использование ресурсов.

Регулярно проверяются данные на официальных сайтах:

Минюст России (списки экстремистских материалов и организаций):
minjust.gov.ru

Роскомнадзор (Единый реестр): eais.rkn.gov.ru

ФСБ России (список террористических организаций): www.fsb.ru

Осторожность.

Не допускается блокировать ресурс самостоятельно или угрожать пользователям. Задача - зафиксировать нарушение и передать информацию уполномоченным органам.

7. ИТОГИ

Эффективное противодействие деструктивной информации в сети «Интернет» обеспечивается органами местного самоуправления при соблюдении следующих условий:

1. Организованности (назначение ответственных, планирование).
2. Бдительности (регулярный мониторинг).
3. Компетентности (знание законодательства и реестров).

4. Оперативности (немедленное информирование территориального отдела прокуратуры и Роскомнадзора).

Следование данным рекомендациям внесет существенный вклад в обеспечение общественной безопасности и защиту прав граждан на территории муниципального образования.