

ИСПОЛЬЗОВАНИЕ КОМПЬЮТЕРНО-ТЕХНИЧЕСКОЙ ЭКСПЕРТИЗЫ ДЛЯ ПОИСКА ЦИФРОВЫХ СЛЕДОВ ЭКСТРЕМИЗМА В ИНТЕРНЕТЕ

Асаёнок Б. В.

Республика Беларусь, г. Минск
Международный университет «МИТСО»,
доцент кафедры уголовно-правовых дисциплин,
кандидат юридических наук, доцент

Фролов Д. Л.

Республика Беларусь, г. Минск
Международный университет «МИТСО»,
магистрант

Современное информационное пространство стало ключевым каналом распространения идей, в том числе экстремистских. Эти идеи способствуют восстановлению в отдельных случаях идеологических предпосылок нацистских и прочих аналогичных им представлений в сознании не только молодежи, но и (через лживую интерпретацию исторических событий и процессов) более широкого круга людей. Такие проявления требуют постоянного внимания и противодействия со стороны государства. Интернет предоставляет возможности для коммуникации, вербовки, пропаганды и координации действий, что делает его удобной средой для противоправной деятельности. В связи с этим особую актуальность приобретает применение компьютерно-технической экспертизы (КТЭ) – комплекса методов анализа цифровых данных, позволяющих выявлять и фиксировать следы экстремистской активности в цифровом пространстве.

Задача экспертизы заключается не только в обнаружении фактов распространения запрещенного контента, но и в обеспечении доказательной базы для правоохранительных органов. Таким образом, КТЭ становится важным инструментом в системе противодействия экстремизму.

Таким образом, основные цели КТЭ в контексте борьбы с экстремизмом:

- ✓ выявление источников распространения экстремистских материалов;
- ✓ установление личности пользователей, участвующих в противоправной деятельности;
- ✓ восстановление удаленных или скрытых данных;
- ✓ анализ цифровых коммуникаций для выявления сетевых связей;
- ✓ формулирование экспертного заключения в качестве источника доказательств по делам об экстремистской деятельности.

Применение КТЭ позволяет решать широкий спектр задач:

- определение IP-адресов, MAC-адресов, уникальных идентификаторов устройств, используемых для распространения экстремистских материалов (в сочетании с методами судебно-лингвистического исследования);
- подготовка материалов к последующему назначению иных судебных экспертиз;
- исследование текстов, изображений, аудио- и видеозаписей на предмет наличия экстремистского содержания, призывов к насилию или пропаганды ненависти (в том числе наличия нацистской символики);
- извлечение удаленных файлов, переписки в мессенджерах, истории браузера и других цифровых следов (к примеру, для определения соответствующих групп пользователей с целью их дальнейшей идентификации);
- определение сетевых контактов между участниками экстремистских групп, выявление каналов коммуникации и координации действий;
- подготовка материалов в форме экспертного заключения, соответствующего нормам уголовно-процессуального законодательства или процессуально-исполнительного законодательства об административных правонарушениях.

Для поиска цифровых следов экстремизма и иных аналогичных противоправных проявлений применяются разнообразные методы:

1. Форензика устройств. Извлечение и анализ данных с жестких дисков, флеш-накопителей, мобильных телефонов. Используются специализированные программы (EnCase, FTK, X-Ways Forensics).
2. Анализ сетевого трафика. Исследование логов серверов, маршрутизаторов и прокси-сервисов для выявления активности подозрительных пользователей.
3. Лингвистический анализ. Применение методов компьютерной лингвистики для выявления экстремистской риторики в текстах, включая использование ключевых слов, семантических моделей и анализа тональности, специфичных для данного направления противоправной деятельности коннотаций.
4. Распознавание изображений и видео. Использование нейросетевых алгоритмов для обнаружения символики экстремистских и националистических организаций, сцен насилия или пропагандистских материалов.
5. Мониторинг социальных сетей. Автоматизированный сбор и анализ данных из открытых источников (OSINT), включая посты, комментарии и переписку в мессенджерах.

Применение КТЭ должно строго соответствовать законодательству в контексте применения норм отраслевых законодательств:

Закон Республики Беларусь «Об оперативно-розыскной деятельности» [1];

Уголовно-процессуальный кодекс Республики Беларусь [2];

Процессуально-исполнительный кодекс Республики Беларусь об административных правонарушениях [3].

Кроме того, при проведении компьютерно-технических исследований актуальным является также обеспечение исполнения законодательства Республики Беларусь о защите персональных данных.

Таким образом, КТЭ является не только технической, но и юридически значимой процедурой, требующей высокой квалификации специалистов.

Рост цифровой активности экстремистских групп делает необходимым постоянное совершенствование методов КТЭ:

1. Искусственный интеллект. Машинное обучение позволяет автоматизировать выявление экстремистских материалов, анализировать большие массивы данных и прогнозировать потенциальные угрозы.

2. Международное сотрудничество. Экстремизм носит транснациональный характер, поэтому обмен опытом и совместные расследования между странами становятся ключевым фактором эффективности.

3. Развитие нормативной базы. Совершенствование законодательства в области цифровой криминалистики обеспечивает правовую основу для применения новых технологий. Здесь следует сказать, что, к сожалению, действующее отраслевое законодательство Республики Беларусь еще слабо продвинулось в регламентации цифровых следов, а также проведении следственных и иных процессуальных действий в цифровом пространстве.

Таким образом, компьютерно-техническая экспертиза является важнейшим инструментом в борьбе с экстремизмом в Интернете, установлении контента, способствующего продвижению нацистской идеологии. Она позволяет выявлять цифровые следы противоправной деятельности, обеспечивать доказательную базу и предотвращать распространение противоправных проявлений такого характера.

Совмещение технических методов и правовых норм делает КТЭ комплексным и эффективным средством противодействия современным угрозам. В условиях стремительного развития цифровых технологий ее значение будет только возрастать, а внедрение искусственного интеллекта и международное сотрудничество откроют новые перспективы в обеспечении безопасности общества.

Список цитированных источников

1. Об оперативно-розыскной деятельности: Закон Респ. Беларусь от 15 июля 2015 г. № 307-3 // ЭТАЛОН: информ.-поисковая система (дата обращения: 11.11.2025).

2. Уголовно-процессуальный кодекс Республики Беларусь: 16 июля 1999 г. № 295-3: принят Палатой представителей 24 июня 1999 г.: одобр. Советом Респ. 30 июня 1999 г.: в ред. Закона Респ. Беларусь от 17 февр. 2025 г. № 61-3 // ЭТАЛОН: информ.-поисковая система (дата обращения: 11.11.2025).

3. Процессуально-исполнительный кодекс Республики Беларусь об административных правонарушениях : 6 янв. 2021 г. № 92-З : принят Палатой представителей 18 дек. 2020 г. : одобр. Советом Респ. 18 дек. 2020 г. / в ред. Закона Респ. Беларусь от 15 апр. 2026 г. № 138-З // ЭТАЛОН : информ.-поисковая система (дата обращения: 11.11.2025).