Е.А. Рабчевский, А.В. Анфалов

Методические рекомендации по методам выявления и оперативного анализа деструктивного контента в сети Интернет с помощью информационно-поисковых систем

СЕУС ЛАБ

УДК 343.34
ББК 67.408.1
Р13

Рабчевский Евгений Андреевич.
Методические рекомендации по методам выявления и оперативного анализа деструктивного контента в сети Интернет с помощью информационно-поисковых систем / Е.А. Рабчевский, А.В. Анфалов. – Пермь, 2024. – 40с.

Методические рекомендации разработаны с целью оказания практической помощи сотрудникам государственных и общественных организаций, осуществляющим информационно-аналитическое обеспечение мероприятий по линии противодействия экстремизму и терроризму, дискредитации Вооруженных Сил и органов публичной власти Российской Федерации, незаконному обороту наркотиков и другим деструктивным явлениям в публичном сегменте сети Интернет.

ISBN - 978-5-6052090-1-0

Оглавление

ОБ АВТОРАХ

Рабчевский Е.А. Основатель и генеральный директор ООО «СЕУСЛАБ». Почетный член Академии военных наук Российской Федерации.

Анфалов А.В. Аналитик ООО «СЕУСЛАБ».

О компании ООО «СЕУСЛАБ»

ООО «СЕУСЛАБ» - российская аккредитованная ИТ-компания. Более 10 лет ведет деятельность в сфере разработки программных решений, предназначенных для информационно-аналитического обеспечения оперативно-разыскной и разведывательной деятельности в сети Интернет (разведка по открытым источникам) на базе технологий Big Data и искусственного интеллекта.

Компания является разработчиком программного комплекса «Поисковая система SEUS», который используется для выявления цифровых следов вовлечения граждан посредством социальных сетей в террористические и экстремистские организации, а также социально-опасные явления (распространение наркотиков, детская порнография, радикальная протестная активность, суицидальное и девиантное поведение, тоталитарные секты и оккультные течения и т.д.).

Компания осуществляет научно-методическое сотрудничество с Антитеррористическим центром государств - участников СНГ (АТЦ СНГ), рядом ВУЗов системы МВД и ФСИН России, Академией военных наук Российской Федерации.

1. ВВЕДЕНИЕ

Методические рекомендации разработаны с целью оказания практической помощи сотрудникам (далее таких сотрудников мы будем называть Операторы) государственных и общественных организаций, осуществляющим информационно-аналитическое обеспечение мероприятий по линии противодействия экстремизму и терроризму, дискредитации Вооруженных Сил и органов публичной власти Российской Федерации, незаконному обороту наркотиков и другим деструктивным явлениям в публичном сегменте сети Интернет.

Деструктивным контентом является вредная информация, размещенная в сети Интернет, обладающая свойствами вирусного распространения и представляющая собой средство противодействия реализации общественно полезных целей и задач государственного управления, определённых в документах стратегического планирования и иных нормативных правовых актах.

В зависимости от причиняемого вреда или потенциальной опасностью его причинения, деструктивный контент может быть противоправным, т.е. информацией, размещенной в сети Интернет, распространение которой запрещено на территории Российской Федерации и подпадает под меры уголовной или административной ответственности.[1]

Деструктивный контент не всегда означает противоправный и в качестве ответных мер за его распространение могут применяться профилактические мероприятия. Куда более предметным и существенным для Оператора является установление противоправного контента, в частности, установление преступлений и правонарушений экстремистской направленности и террористического характера. В соответствии с Федеральными законами от 25 июля 2002 года № 114-ФЗ «О противодействии экстремистской деятельности» и от 6 марта 2006 года № 35-ФЗ «О противодействии терроризму» на территории Российской Федерации запрещается распространение экстремистских и

1 - Деструктивный контент: понятие, административно-правовая характеристика, виды. / К.А. Шуликов // Санкт-Петербург: Вестник Нижегородского университета им. Н.И. Лобачевского, 2023 № 2 с. 176-182 DOI 10.52452/19931778_2023_2_176

террористических материалов. За нарушение запрета предусмотрена уголовная и административная ответственность.

Для выявления преступлений и правонарушений, указанных выше, необходимо точно понимать какие организации и материалы признаны экстремистскими и террористическими и запрещены на территории Российской Федерации.

Список запрещенных материалов формирует Минюст России на основании решений судов и размещен на официальном сайте.[2] Организации, признанные на территории Российской Федерации экстремистскими и террористическими, отражены в Едином федеральном списке организаций, в том числе иностранных и международных организаций, признанных в соответствии с законодательством Российской Федерации террористическими. Актуальный список размещен на сайтах Национального антитеррористического комитета России.[3]

Многие деструктивные темы уже подпадают под правовое регулирование. Выделяются следующие направления деструктивного контента, представляющие потенциальную угрозу безопасности государства и общества:

- пропаганда или оправдание террористической или экстремистской деятельности (ст. 205.2 УК РФ);
- склонение, вербовка, финансирование или иное вовлечение лиц в совершение террористических преступлений (ст. 205.1 УК РФ);
- организация экстремистских сообществ и деятельности экстремистских организаций, их финансирование (ст. 282.1 УК РФ, ст. 282.2 УК РФ, ст. 282.3 УК РФ);
- распространение информации об организации, объединении, признанной на территории Российской Федерации экстремистской; производство и распространение экстремистских материалов (ч. 2 ст. 13.15 КоАП РФ, ст. 20.29 КоАП РФ);

2 - https://minjust.gov.ru/ru/extremist-materials (дата обращения: 26.04.2024).
3 - http://nac.gov.ru/terroristicheskie-i-ekstremistskie-organizacii-i-materialy.html (дата обращения: 26.04.2024).

- призывы или оправдания действий, оскорбляющих религиозные чувства верующих (ст. 148 УК РФ);
- пропаганда или призывы к подрыву суверенитета и нарушению территориальной целостности государства (ст. 280.1 УК РФ);
- разжигание расовой и этнической ненависти, либо вражды (ст. 20.3.1 КоАП РФ, ст. 282 УК);
- пропаганда или призывы насильственного изменения конституционного строя;
- склонение, вербовка или иное вовлечение лиц в массовые беспорядки (ст. 212 УК РФ);пропаганда или реабилитация нацисткой идеологии, (ст. 354.1 УК РФ);
- пропаганда, либо публичное демонстрирование нацистской атрибутики, атрибутики и символики экстремистских организаций (ст. 20.3 КоАП РФ);
- дискредитация использования Вооруженных Сил Российской Федерации в целях защиты интересов Российской Федерации и ее граждан, поддержания международного мира (ст. 20.3.3 КоАП РФ, ст. 280.3 УК РФ);
- пропаганда или призывы к развязыванию межгосударственных или внутренних войн;
- осквернение исторической памяти, символов воинской славы или государственных символов;
- пропаганда порнографических материалов, связанных с несовершеннолетними, а также оскорбляющих честь и достоинства человека;
- пропаганда наркотических средств, психотропных веществ или их прекурсоров (ст. 6.13 КоАП РФ);
- призывы к возбуждению ненависти, вражды или нарушению общепринятых норм поведения;

- пропаганда или оправдание преступной деятельности и криминальной идеологии.

На практике деятельность Оператора по выявлению и анализу деструктивных материалов в сети Интернет зачастую именуется «Мониторингом сети Интернет» и может быть структурирована на следующие основные этапы работы:

1. Формирование набора поисковых признаков по интересующей Оператора тематике;
2. Занесение поисковых признаков в информационно-поисковую систему;
3. Поиск/сбор оперативно-значимых материалов;
4. Установление лиц, разместивших материалы, в том числе авторов, использующих способы конспирации при распространении контента;
5. Оценка собранной информации применительно к решаемым задачам.

Перечисленные этапы осуществляются последовательно, но для повышения эффективности рекомендуется осуществлять их в итерационном порядке, периодически по мере поступления новой информации возвращаясь к предыдущим этапам для формирования и отработки новых версий.

На всех этапах осуществляется проверка актуальности и достоверности полученных первичных данных.

Необходимо принять во внимание, что основными факторами при выборе злоумышленником каналов распространения деструктивной информации являются:

- способность быстрого вовлечения широких масс населения в потребление деструктивного контента (ключевой фактор);
- сохранение анонимности автора контента;

- простота (дешевизна) и скорость размещения контента.

Интернет-СМИ подвержены широкому государственному регулированию, в частности со стороны Роскомнадзора, и с точки зрения злоумышленника, за редким исключением, интереса не представляют.

Интернет-сайты требуют большего количества временных ресурсов для размещения контента и без серьезных затрат на интернет-маркетинг не дают возможности воздействовать на широкие массы интернет-аудитории, поэтому также редко используются злоумышленниками.

С учетом указанных выше факторов приоритетными каналами для распространения деструктивной информации в сети Интернет являются социальные сети и мессенджеры. В связи с этим, данные рекомендации в значительной степени будут ориентированы на работу с социальными сетями и мессенджерами.

2. МЕТОДИКА РЕАЛИЗАЦИИ ЭТАПОВ МОНИТОРИНГА СЕТИ ИНТЕРНЕТ

2.1. Формирование набора поисковых признаков

Процесс сбора первичной информации следует начать с выявления деструктивного контента по тематике, интересующей Оператора.

Анализ деструктивных течений представляет из себя многоступенчатый итерационный процесс, в ходе которого на основании первичных поисковых признаков в результате целенаправленного поиска могут порождаться вторичные поисковые признаки. Для формирования тематик поисковых признаков необходимо опираться на действующее законодательство по линии противодействия экстремизму и терроризму и осведомленности о видах и особенностях деструктивных течений. Данный процесс также строится с учетом проработки различных версий, в ходе отработки которых проверяются различные поисковые признаки. Таким образом набор поисковых признаков для заданного деструктивного явления постепенно уточняется и дополняется.

Поисковые признаки могут быть следующих видов:

1. Контент

1.1. Лингвистические поисковые признаки

1.1.1. Характерная лексика, например:

- Словоформы или терминология (слэнг), используемые вовлеченными лицами и характеризующие явление (субкультуру/движение).
- Сведения об идеологах, функционерах деструктивных явлений.
- Тексты цитат, используемые лицами, вовлеченными в деструктивное явление (субкультуру/движение).

- Заголовки текстовых материалов, произведений, интернет-фольклора и их авторов.
- Транскрипты (тексты) песен, авторы, названия групп, используемые лицами, вовлеченными в деструктивное явление.
- Заголовки, описание видеоконтента, используемые лицами, вовлеченными в деструктивное явление.
- Текстовые аббревиатуры, используемые лицами, вовлеченными в деструктивное явление.
- Цифровые устойчивые символы, характерные для деструктивных явлений.
- Спецсимволы, характерные для деструктивного явления (卐, 卍, ✙, ϟϟ и т.д.).
- Текст ссылок, содержащий сочетания символов, характеризующих деструктивное явление/событие.
- Наименование брендов и моделей.

1.1.2. Характерные даты, например:

- Даты совершения каких-либо резонансных преступлений.
- Даты рождения и смерти идеологов и основных функционеров деструктивных явлений.

1.1.3. Сетевые, финансовые реквизиты, установочные данные и другая оперативная информация по уже имеющимся объектам интереса, например:

- Номера счетов преступных организаций, распространяемые для сбора средств (QIWI- Bitcoin-кошельки).
- Номера телефонов для связи.

- Адреса электронной почты для связи, логины и прочая информация о способах связи.

1.2. Поисковые признаки на изображениях

1.2.1. Изображения лиц, например:

- Изображения лиц лидеров и идеологов деструктивных явлений.
- Изображения лиц функционеров деструктивных явлений.
- Изображения лиц последователей деструктивных явлений.

1.2.2. Изображения, содержащие характерную символику, например:

- Символика запрещенных экстремистских и террористических организаций, в том числе флаги, логотипы и прочее.
- Характерные мемы.

1.2.3. Изображения, содержащие характерные предметы, например:

- Орудия убийства и прочих оккультных и псевдорелигиозных ритуалов.

1.2.4. Изображения, на которых содержится текст, соответствующий лингвистическим поисковым признакам

1.2.5. Фотографии мест, представляющих оперативный интерес, например:

- Фотографии с мест совершения резонансных преступлений.
- Фотографии с мест каким-либо образом связанных с проживанием, образовательной, профессиональной

или другой деятельностью объекта интереса или лиц, олицетворяющих деструктивное явление, в том числе, их памятники и мемориалы.

1.3. Поисковые признаки в аудиозаписях

- Аудиозаписи, включенные в федеральный список экстремистских материалов.
- Аудиозаписи, содержащие лингвистические признаки пропаганды, вовлечения в деструктивные течения и экстремистские, террористические организации.
- Аудиозаписи, содержащие слэнг, цитаты, используемые лицами, вовлеченными в деструктивные явления.
- Аудиозаписи, авторами, исполнителями которых являются лидеры, идеологи и функционеры деструктивных явлений.

1.4. Поисковые признаки в видеозаписях

2.1.1. Видеозаписи, включенные в федеральный список экстремистских материалов.

2.1.2. Видеозаписи, по своему смыслу имеющие признаки пропаганды, либо вовлечения в экстремистские, террористические организации и деструктивные явления, содержащие:

- Изображения лидеров, идеологов и функционеров деструктивных явлений.
- Изображения атрибутики, символики экстремистских, террористических организаций и деструктивных явлений.
- Слэнг, цитаты, используемые лицами, вовлеченными в деструктивные явления.
- Сетевые, финансовые реквизиты, установочные данные и другая оперативная информация по уже имеющимся объектам интереса.

- Аудиозаписи, включенные в федеральный список экстремистских материалов.

2. Связи с имеющимися объектами интереса, например:

- Связи типа «дружба/подписка»
- Связи на основании оставленных комментариев и отметок «нравится» и других
- Связи на основании делаемых репостов и пересылки материалов
- Связи на основании отметок присутствия на фото
- Связи нескольких пользователей на основании выявления присутствия их на совместном фото
- Связи на основании приглашения одного пользователя в чат другим
- Связи на основании работы или обучения в одном заведении, занятия в одних секциях, совместного участия в мероприятиях

3. Геолокационные данные, представляющие оперативный интерес, например:

- Координаты мест совершения резонансных преступлений
- Координаты мест, каким-либо образом связанных с проживанием, образовательной, профессиональной или другой деятельностью объекта интереса или лиц, олицетворяющих деструктивное явление

4. Внешние признаки:

- Характерные виды прически
- Характерные татуировки
- Характерные фасоны одежды и способы ее ношения

Перечисленные виды поисковых признаков должны формироваться Оператором на основе складывающейся обстановки, могут значительно отличаться в зависимости от территорий и поставленных задач.

2.2. Занесение поисковых признаков в информационно-поисковую систему

Поисковые признаки могут формироваться Оператором самостоятельно или быть заранее заложенными в информационно-поисковую систему (далее ИПС) их разработчиками.

Два различных подхода к вопросу определения процесса формирования поисковых признаков нашли реализацию в различных ИПС.

Широкую практику получил метод поиска на основе лингвистических поисковых признаков, который реализуется в поисково-аналитических инструментах в виде поиска по текстовому запросу (Оператор делает запрос в информационной системе самостоятельно), либо поиск осуществляется сразу по целому набору текстовых запросов в виде «словаря», отражающего область интереса Оператора.

В современных ИПС такие запросы обрабатываются достаточно быстро (от нескольких секунд до минут в зависимости от сложности и «тяжести» запроса). Это дает Оператору возможность максимально оперативно проверять разные версии, получать новые поисковые признаки и т.д.

2.3. Поиск/сбор оперативно значимых материалов

По поисковым признакам в ИПС осуществляется поиск первичной информации, которая представляет из себя опубликованные материалы с сопутствующими метаданными. Метаданные используются в последующем для установления объекта интереса, определения актуальности и достоверности оперативно значимых материалов. Дается первичная правовая оценка выявленным материалам.

Реализация данного этапа также имеет различные подходы в зависимости от используемых инструментов. Рассмотрим их подробнее в следующих разделах.

2.3.1. Подход технологий больших данных

Данный подход предполагает два аспекта:

1. ИПС автоматически на постоянной основе осуществляет сбор данных (собираются все доступные данные, а не только те, которые соответствуют поисковым признакам).

2. Собираемые данные сохраняются в специализированные центры обработки данных (далее ЦОД). А доступ к данным, которые соответствуют поисковым признакам, осуществляется к их копиям, сохраненным в ЦОД.

Подход использования технологий больших данных предоставляет Оператору следующие преимущества:

- Полный объем информации из социальной сети;
- Поиск и отображение информации удаленной/измененной пользователями соц. сетей;
- Отслеживание изменений (версионности) метаданных профилей пользователей социальных сетей (ФИО, география и другие параметры);
- Получение набора публикаций, выполненных конкретным пользователем социальной сети (не только на странице пользователя, но и во всем информационном пространстве).

Вместе с тем работа с информационными системами, реализующими подход больших данных, требует от Оператора определенной квалификации в виде знания основ информационного поиска и навыков аналитической обработки информации.

От производителя информационной системы применение

подхода больших данных требует существенных затрат на создание и содержание ЦОД.

2.3.2. Подход узкого тематического мониторинга

Другим возможным подходом к реализации сбора данных является вариант, когда сбор данных осуществляется непосредственно с рабочего компьютера Оператора.

В этом случае осуществляется сбор лишь тех данных, которые на момент сбора размещены в сети Интернет и соответствуют конкретным поисковым признакам. При этом для фильтрации информации по поисковым признакам используются внутренние механизмы информационных площадок (социальной сети, мессенджера), на которых осуществляется поиск. Механизмы фильтрации информационных площадок предназначены для обычных пользователей социальных сетей. Вследствие этого фильтрация не дает возможности реализации всех видов поисковых признаков и значительно ограничена по объемам предоставляемой информации.

Кроме того, такой подход сопряжен с рядом рисков и недостатков:

- Риск раскрытия сетевых реквизитов Оператора не только производителю ИПС, но и администрации информационных площадок, на которых осуществляется поиск;
- Малый объем получаемых данных из-за ограничений в механизмах поисковой выдачи информационных площадок. Например, социальная сеть «ВКонтакте» выдает не более 1000 результатов на один запрос;
- Ограничения информационной площадки по количеству и объему запросов в связи с анти-DDoS защитой (защита от слишком интенсивного осуществления поисковых запросов);

- Отсутствие возможностей «тонкой» настройки запросов под соответствие поисковым признакам из-за использования ограниченных механизмов поиска самих информационных площадок.

Вместе с тем реализация такого подхода не требует огромных затрат на содержание ЦОД и в то же время в целом отвечает общему порядку информационно-аналитической работы Оператора.

2.3.3. Подход тематического мониторинга с применением технологий больших данных

Данный подход по назначению больше направлен на задачи мониторинга информации, а не целенаправленного поиска, но при этом использование технологий больших данных позволяет получить Оператору некоторые преимущества, указанные в разделе 2.3.1.

Информационно-поисковая система сама на постоянной основе осуществляет сбор данных, но в отличие от подхода 2.3.1 Оператору доступны для обработки не все данные, а только те, которые соответствуют поисковым признакам, заложенным в ИПС её разработчиком. В этом случае собираемые данные также сохраняются в специализированные центры обработки данных.

Преимущества подхода:

- Получение информации в режиме реального времени;
- Автоматизированное формирование отчетов по полученной информации.

Недостатки подхода:

- Ограниченность информационной выдачи параметрами, заданными производителем ИПС;
- Невозможность формирования и корректировки поисковых признаков Оператором самостоятельно во время работы в ИПС «на лету»;
- Временные задержки на связь с производителем ИПС для

формирования и изменения набора поисковых признаков;

Информационные системы, созданные с применением данного подхода предназначены в первую очередь для Операторов, которым необходим оперативный мониторинг информационной обстановки по различным направлениям.

2.3.4. Подход объектового анализа

Подход объектового анализа предполагает сбор данных с отдельного вынесенного сервера. При этом данные собираются в большей мере не сколько из социальных сетей и мессенджеров, сколько из агрегаторов различных источников данных, которые способствуют установлению личности аккаунтов, представляющие интерес. Таким образом, данный подход дополняет результаты работы, которые выполняются с помощью подходов 2.3.1 или 2.3.2, 2.3.3.

К дополнительным плюсам данного подхода можно отнести снижение риска раскрытия сетевых реквизитов Оператора. Эта информация остается доступна только производителю ИПС, а агрегаторы данных могут фиксировать лишь сетевые реквизиты серверов производителя ИПС.

2.4. Установление лиц, разместивших материалы

Открытые источники данных в глобальной сети Интернет позволяют получать разнообразную информацию об объектах интереса. К открытым источникам относятся не только социальные сети и мессенджеры, но и различные базы данных, размещенные в онлайн - пространстве. После выявления деструктивного контента в сети Интернет ключевым этапом является установление лица – автора противоправных материалов экстремистского и террористического характера.

Изучение аккаунта пользователя соцмедиа позволяет получить значимые сведения как доказательственного, так и ориентирующего характера. Процесс сбора информации о пользователе

осуществляется с целью установления владельца аккаунта и получения характеризующей информации о пользователе (объекте интереса).

С применением информационно-поисковых систем в значительной мере повышается эффективность получения установочных данных и представляется возможным создать «цифровой портрет» путем сбора характеризующих материалов, анализа активности в социальных сетях и мессенджерах.

Профиль пользователя соцмедиа может включать в себя два вида информации:

1. Основные данные о профиле:

    1.1. ФИО, дата рождения, семейное положение, география и адреса проживания, места работы и должности, сведения об образовании и другие;

    1.2. Реквизиты документов объекта интереса: паспортные данные, СНИЛС, водительское удостоверение и другие;

    1.3. Контактные данные: номера телефонов, адреса электронных почт и другое;

    1.4. Данные об имуществе: vin, государственный номер зарегистрированного на объект автомобиля, сведения о недвижимости и другое;

    1.5. Биометрические данные: фотоизображения объекта интереса и его окружения;

    1.6. Финансовые реквизиты: номера электронных кошельков, банковских карт и другое.

2. Данные о сетевой активности профиля:

    2.1. Сетевые реквизиты объекта: профили в социальных сетях, мессенджерах, иных web-сервисах, время входа;

    2.2. Социальные связи объекта;

2.3. Сведения о вовлеченности объекта интереса в различные события/явления;

2.4. Сведения об аффилированности объекта интереса с различными людьми/организациями.

Перечень сведений для установления владельца аккаунта и получения характеризующей информации о нем, которые могут быть установлены из открытых источников, а также соответствующие методы получения информации приведены в Таблица 1:

Информация о профиле	**Метод установления с помощью информационно-поисковых систем**
ФИО	• Изучение анкетных данных профиля автора в социальной сети, с которого происходило распространение деструктивной информации; • Анализ активности автора в социальной сети (указание данных в постах и комментариях на страницах сообществ и пользователей (например, обращение к автору по имени; указание персональных данных при утрате документов); • Получение информации из дополнительных открытых источников данных по иным параметрам установленной информации; • Поиск аккаунтов в других соцмедиа по иным параметрам установленной информации.

Информация о профиле	**Метод установления с помощью информационно-поисковых систем**
Дата рождения	• Изучение анкетных данных профиля автора в социальной сети, с которого происходило распространение деструктивной информации; • Анализ активности автора в социальной сети (поздравления с днем рождения другими пользователями, посты самого автора); • Получение информации из дополнительных открытых источников данных по иным параметрам установленной информации; • Поиск аккаунтов и их изучение в других соцмедиа по иным параметрам установленной информации.

Информация о профиле	**Метод установления с помощью информационно-поисковых систем**
Место проживания	• Изучение анкетных данных профиля автора в социальной сети, с которого происходило распространение деструктивной информации (при отсутствии данных о географии в анкете вывод можно сделать по данным об образовании (город указанной школы, ВУЗа, СУЗа и т.д.), месте работы и т.д. Если указан сотовый телефон, то с высокой долей вероятности можно определить регион); • Анализ активности автора в социальной сети (например, активность в сообществе района); • Изучение региональных, городских, районных сообществ, либо любых других с указанием географии, в которых состоит автор (например, региональных спортивных клубов); • Изучение географии «друзей» автора; • Анализ видеозаписей и фотоконтента, размещенного на странице автора; • Получение информации из дополнительных открытых источников данных по иным параметрам установленной информации; • Поиск аккаунтов и их изучение в других соцмедиа по иным параметрам установленной информации.

Информация о профиле	**Метод установления с помощью информационно-поисковых систем**
Место работы, должность	• Изучение анкетных данных профиля автора в социальной сети, с которого происходило распространение деструктивной информации; • Анализ активности автора в социальной сети (например, активность в профессиональных сообществах, комментарии с критикой руководства и т.д.); • Изучение сообществ, в которых состоит автор (например, сообщество завода); • Изучение кластера друзей автора на графе («друзья» автора, являющиеся коллегами); • Анализ видеозаписей и фотоконтента, размещенного на странице автора (фотографии с профессиональных мероприятий, в рабочей одежде); • Получение информации из дополнительных открытых источников данных по иным параметрам установленной информации; • Поиск аккаунтов и их изучение в других соцмедиа по иным параметрам установленной информации.

Информация о профиле	**Метод установления с помощью информационно-поисковых систем**
Сведения об образовании	• Изучение анкетных данных профиля автора в социальной сети, с которого происходило распространение деструктивной информации; • Анализ активности автора в социальной сети (например, активность в сообществах ВУЗа, класса и т.д.); • Изучение сообществ, в которых состоит автор (например, сообщество СОШ); • Изучение кластера друзей автора на графе («друзья» автора, предположительно являющиеся одноклассниками, одногруппниками); • Анализ видеозаписей и фотоконтента, размещенного на странице автора (например, фотографии с публичных мероприятий ВУЗа); • Получение информации из дополнительных открытых источников данных по иным параметрам установленной информации; • Поиск аккаунтов и их изучение в других соцмедиа по иным параметрам установленной информации.

Информация о профиле	**Метод установления с помощью информационно-поисковых систем**
Семейное положение, состав семьи	• Изучение анкетных данных профиля автора в социальной сети, с которого происходило распространение деструктивной информации; • Анализ активности в сообществах детских садов, школ и т.д.; • Анализ однофамильцев среди друзей; • Лайки, репосты, реакции на странице автора и других пользователей; • Изучение кластера друзей автора на графе («друзья» автора, являющиеся одноклассниками, одногруппниками); • Изучение фотографий и видеозаписей с другими пользователями в истории аватаров и фотоконтенте (фотографии с семейных торжеств); • Получение информации из дополнительных открытых источников данных по иным параметрам установленной информации; • Поиск аккаунтов и их изучение в других соцмедиа по иным параметрам установленной информации.

Информация о профиле	**Метод установления с помощью информационно-поисковых систем**
Реквизиты документов: паспортные данные, СНИЛС, водительское удостоверение и другие	• Анализ активности в сообществах (например, «Подработка», «Шабашка» и т.д.); • Изучение фотографий; • Получение информации из дополнительных открытых источников данных по иным параметрам установленной информации; • Поиск аккаунтов и их изучение в других соцмедиа по иным параметрам установленной информации.
Информация о профиле	**Метод установления с помощью информационно-поисковых систем**
Номера телефонов, адреса электронных почт и другое	• Изучение анкетных данных профиля автора в социальной сети, с которого происходило распространение деструктивной информации; • Анализ активности автора в социальной сети; • Получение информации из дополнительных открытых источников данных по иным параметрам установленной информации; • Поиск аккаунтов в других соцмедиа по иным параметрам установленной информации.

Информация о профиле	**Метод установления с помощью информационно-поисковых систем**
Данные об имуществе: vin, государственный номер зарегистрированного на объект автомобиля, сведения о недвижимости и другое	• Анализ активности автора в социальной сети; • Изучение фотографий и видеозаписей автора (фотографии с автомобилем); • Получение информации из дополнительных открытых источников данных по иным параметрам установленной информации; • Поиск аккаунтов в других соцмедиа по иным параметрам установленной информации.
Информация о профиле	**Метод установления с помощью информационно-поисковых систем**
Биометрические данные: фотоизображения объекта интереса и его окружения	• Анализ фотоконтента и видеозаписей, размещенных на странице автора и его друзей; • Получение информации из дополнительных открытых источников данных по иным параметрам установленной информации; • Поиск аккаунтов и их изучение в других соцмедиа по иным параметрам установленной информации.

Информация о профиле	Метод установления с помощью информационно-поисковых систем
Финансовые реквизиты: номера электронных кошельков, банковских карт и другое	• Анализ активности автора в социальной сети; • Анализ фотоконтента, размещенного на странице автора; • Получение информации из дополнительных открытых источников данных по иным параметрам установленной информации; • Поиск аккаунтов и их изучение в других соцмедиа по иным параметрам установленной информации.
Информация о профиле	**Метод установления с помощью информационно-поисковых систем**
Сетевые реквизиты объекта: профили в социальных сетях, мессенджерах, иных web сервисах, время входа	• Изучение анкетных данных профиля автора в социальной сети, с которого происходило распространение деструктивной информации; • Анализ времени присутствия в сети (сопоставление дат и времени вхождений, активности автора с жизненными событиями предполагаемого лица); • Получение информации из дополнительных открытых источников данных по иным параметрам установленной информации; • Поиск аккаунтов в других соцмедиа по иным параметрам установленной информации.

Информация о профиле	**Метод установления с помощью информационно-поисковых систем**
Социальные связи объекта	• Анализ активности на страницах других пользователей; • Изучение кластеров «друзей» автора (например, путем графовых технологий); • Анализ взаимодействия автора с другими пользователями - лайки, репосты, реакции на странице автора и других пользователей; • Изучение фотографий и видеозаписей с другими пользователями в истории аватаров и фото-, видеоконтенте; • Поиск аккаунтов и их изучение в других соцмедиа по иным параметрам установленной информации.

Информация о профиле	**Метод установления с помощью информационно-поисковых систем**
Сведения о вовлеченности объекта интереса в различные события/явления	Установление поисковых признаков путем: • Изучения анкетных данных автора в социальной сети, с которого происходило распространение деструктивной информации (поля анкетных данных «статус», «интересы» и т.д.) • Анализа активности автора в социальной сети (например, активность в сообществах деструктивных течений); • Изучения сообществ, в которых состоит автор; • Изучения «друзей» автора, анализ общих с автором сообществ («Навальный», «Рёдан» и т.д.); • Анализа видеозаписей и фотоконтента, размещенного на странице автора; • Анализ аудиозаписей; • Поиск аккаунтов и их изучение в других соцмедиа по иным параметрам установленной информации.

Информация о профиле	**Метод установления с помощью информационно-поисковых систем**
Сведения о вовлеченности объекта интереса в различные события/явления	• Изучение анкетных данных автора в социальной сети, с которого происходило распространение деструктивной информации; • Анализ активности автора в социальной сети; • Изучение сообществ, в которых состоит автор; • Изучение кластера друзей автора (например, путем графовых технологий); • Анализ видеозаписей и фотоконтента, размещенного на странице автора (например, фотографии с профессиональных мероприятий); • Получение информации из дополнительных открытых источников данных по иным параметрам установленной информации; • Поиск аккаунтов и их изучение в других соцмедиа по иным параметрам установленной информации.

Данные методы применяются для установления владельца аккаунта, являющегося автором деструктивного или противоправного контента. Когда Оператор обнаруживает лицо, участвовавшее, например, в несанкционированном мероприятии, либо совершившего диверсию и т.д., одним из ключевых шагом является анализ социальных сетей данного лица. Поиск аккаунтов лица и получение характеризующей информации можно получить исходя из вышеперечисленных методов.

При проведении аналитической работы важна как каждая деталь, так и все данные в совокупности.

2.5. Оценка собранной информации применительно к решаемым задачам

2.5.1. Действия Оператора при обнаружении деструктивных, экстремистских и террористических материалов:

- Выявление материалов с признаками деструктивных, экстремистских, либо террористических течений в сети Интернет путем ручного поиска, либо с использованием информационно-поисковых систем.
- При установлении деструктивных материалов без признаков преступлений и правонарушений - проведение профилактической работы (см. п.2.5.2).
- Провести предварительную проверку материалов на наличие признаков экстремистских материалов, наличие их в федеральном списке экстремистских материалов, причастности лица к экстремистским, террористическим организациям.
- Принять меры по установлению лиц, причастных к совершению правонарушения, преступления (распространению, производству, хранению).
- При наличии признаков преступлений или правонарушений необходимо подготовить рапорт и доложить руководству.

2.5.2. Профилактические мероприятия, проводимые Оператором при обнаружении деструктивных материалов

Для эффективного мониторинга социальных сетей и проверки лиц на предмет приверженности деструктивным течениям необходимо постоянно изучать тенденции в появлении новых субкультур, оценивать их привлекательность для несовершеннолетних и молодежи, лиц наиболее подверженных деструктивным проявлениям. Это важно для предотвращения распространения негативного влияния на молодое поколение.

Для достижения этой цели необходимо постоянно поддерживать в ИПС в актуальном состоянии основные поисковые признаки, связанные с различными тематиками. Это позволит эффективно выявлять потенциально деструктивные материалы, которые могут нанести вред. Важно отметить, что мониторинг социальных сетей должен быть постоянным и систематическим процессом. Такой подход позволит более эффективно реагировать на потенциальные угрозы и предотвращать негативные последствия.

Не менее важным шагом является участие Оператора в профилактических мероприятиях в учебных заведениях совместно с сотрудниками ПДН (правоохранительных органов), КДН (комиссии по делам несовершеннолетних) и представителями Координационных центров по вопросам формирования у молодежи активной гражданской позиции, предупреждения межнациональных и межконфессиональных конфликтов, противодействия идеологии терроризма и профилактики экстремизма с педагогическим составом учебных заведений. В рамках этих мероприятий проводятся лекции об основных деструктивных течениях, которые представляют опасность для молодежи.

При выявлении признаков деструктивных течений у лица следует установить контроль за их поведением и принять меры для исключения возможности дальнейшего распространения деструктивных течений, при необходимости провести профилактическую беседу.

Особое внимание следует уделять уровню профессиональной

компетенции специалистов, которые работают непосредственно с несовершеннолетними и молодыми людьми, находящимися в группе риска. Часто профессионалы, занимающиеся этой работой, не всегда готовы к взаимодействию с проблемными подростками и молодыми людьми. Поэтому важно осуществлять коррекцию в данной области и внедрять новые принципы педагогической работы, психологические практики, чтобы эффективно справляться с вызовами и потребностями данной группы молодежи.

3. ЗАКЛЮЧЕНИЕ

Подводя итоги, отметим, что рамки настоящего документа не позволили подробно описать все тонкости применения средств автоматизации по выявлению и анализу деструктивных материалов в социальных сетях и мессенджерах. Кроме того, работа (применение настоящих методик) Оператора сильно зависит от доступных Оператору инструментов автоматизации, т.е. от использования конкретных ИПС.

Из опыта авторов, наилучшие результаты приносят ИПС, основанные на технологиях больших данных. Но их более широкое практическое применение сдерживают высокие затраты на создание и эксплуатацию соответствующих центров обработки данных из-за требований к вычислительным мощностям и объемам хранимых данных порядка нескольких Петабайт.

На настоящий момент ни одна из существующих отечественных ИПС не способна надёжно покрыть решение всех задач в области выявления и оперативного анализа деструктивного контента. У каждой известной ИПС есть свои достоинства и недостатки, поэтому наилучшим вариантом представляется параллельное применение оптимального набора ИПС (из числа зарекомендовавших себя решений) от разных производителей, чтобы результаты разных ИПС эффективно дополняли друг друга.

Авторы планируют в будущем продолжить начатую работу по созданию серии методических руководств по применению средств автоматизации в решении задач противодействия деструктивным и противоправным явлениям в публичном сегменте сети Интернет.

Методические рекомендации

Рабчевский Евгений Андреевич
Анфалов Александр Викторович

Методические рекомендации по методам выявления и оперативного анализа деструктивного контента в сети Интернет с помощью информационно-поисковых систем

Оформление и верстка:
ООО «СЕУСЛАБ»

Подписано в печать: 15.04.2024 г.
Формат 60x90/16, бум. ВХИ 80гр, усл.печ.л. 2,25
Тираж 100 экз., заказ 296755
Отпечатано в типографии
ИП Левин В.А. (Группа предприятий «Астер»).
614000, г. Пермь, ул. Усольская, 15