Методические рекомендации по мониторингу противоправных материалов в сети «Интернет» (кибербуллинг, материалы экстремистской направленности)

Курск, 2021 г.

СОДЕРЖАНИЕ

Введение

В данных методических рекомендациях содержится информация о способах мониторинга социальных сетей для поиска материалов экстремистской направленности, кибербуллинга и лиц, предположительно, занимающихся вербовкой молодых людей в запрещенные на территории Российской Федерации (далее - РФ) организации.

Основные направления деятельности:

1. Мониторинг сети «Интернет» на предмет выявления материалов, предположительно, экстремистской направленности;
2. Мониторинг сети «Интернет» на предмет кибербуллинга;
3. Мониторинг сети «Интернет» на предмет выявления лиц, предположительно, занимающихся вербовкой молодых людей в запрещенные на территории РФ организации;
4. Размещение в социальных сетях позитивного контента.

Информация для эксперта, занимающегося мониторингом, и постороннего человека, обнаружившего негативный контент

Эксперт должен быть морально готов к негативному контенту различного характера, так как проводит мониторинг сообществ и страниц, которые разделяют радикальные идеологии, занимаются целенаправленной вербовкой людей и т.д.

1. Эксперт при проведении мониторинга на наличие противоправного контента должен следить за режимом времени мониторинга, делать перерывы на отдых, отвлекаться просмотром позитивного контента.
2. Необходимо обсуждать с коллегами найденную информацию и результаты, которых удалось достичь. В процессе обсуждения происходит психологическая разгрузка. Все выявленные материалы необходимо незамедлительно передавать вашему руководству, после чего сохраненный материал необходимо удалить. Запрещается использование выявленных материалов в иных целях, их хранение на личных цифровых носителях, распространение или передача третьим лицам.

Правила по основам мониторинга социальных сетей

1. В рамках мониторинга осуществляйте просмотр групп, которые вызывают интерес у молодежи, склонной к радикальным настроениям: праворадикальные группы, группы с пропагандой радикального ислама и др.
2. Весь найденный деструктивный контент следует фиксировать на скриншотах или же делать фото экрана. Часто бывает, что администраторы и участники экстремистских сообществ удаляют информацию с сайтов. В данном случае, если контент не был зафиксирован, впоследствии невозможно доказать, что на сайте присутствовал опасный и противоправный контент.

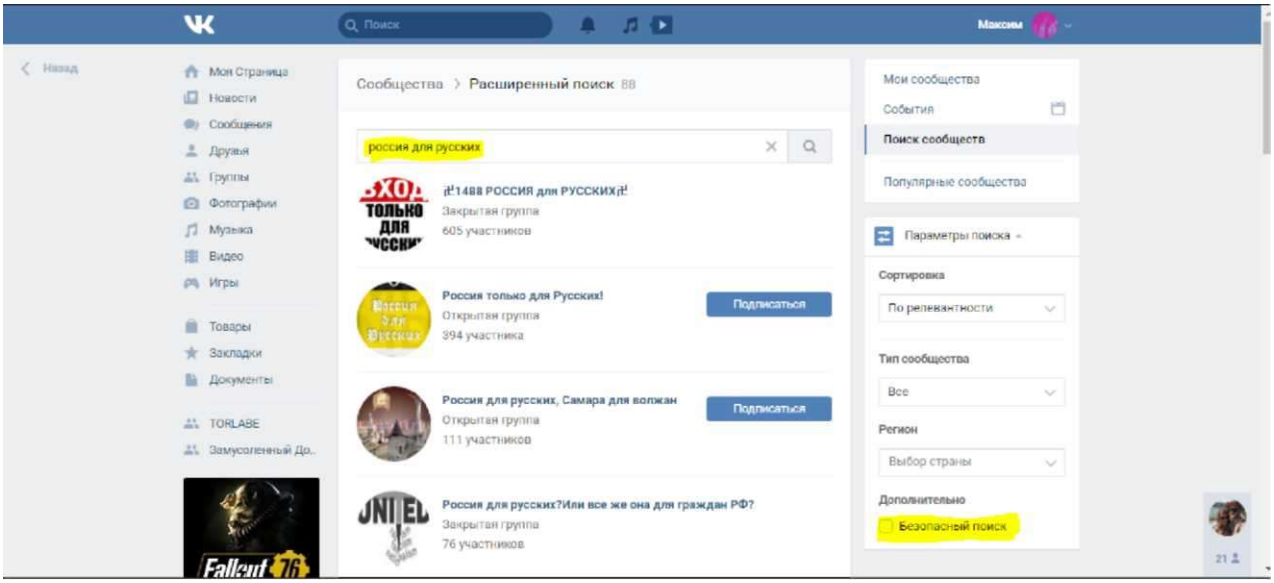
3. Запрещено вступать в контакт с лицами, предположительно, занимающимися вербовкой молодых людей в запрещенные на территории РФ организации, и лицами, которые явно связаны с экстремистскими течениями. При нахождении противоправной информации по итогам мониторинга составьте отчет и направьте его согласно схемам, представленным далее.

4. Незамедлительно передавайте выявленную информацию руководителям и отделению безопасности ОБПОУ «КБМК».

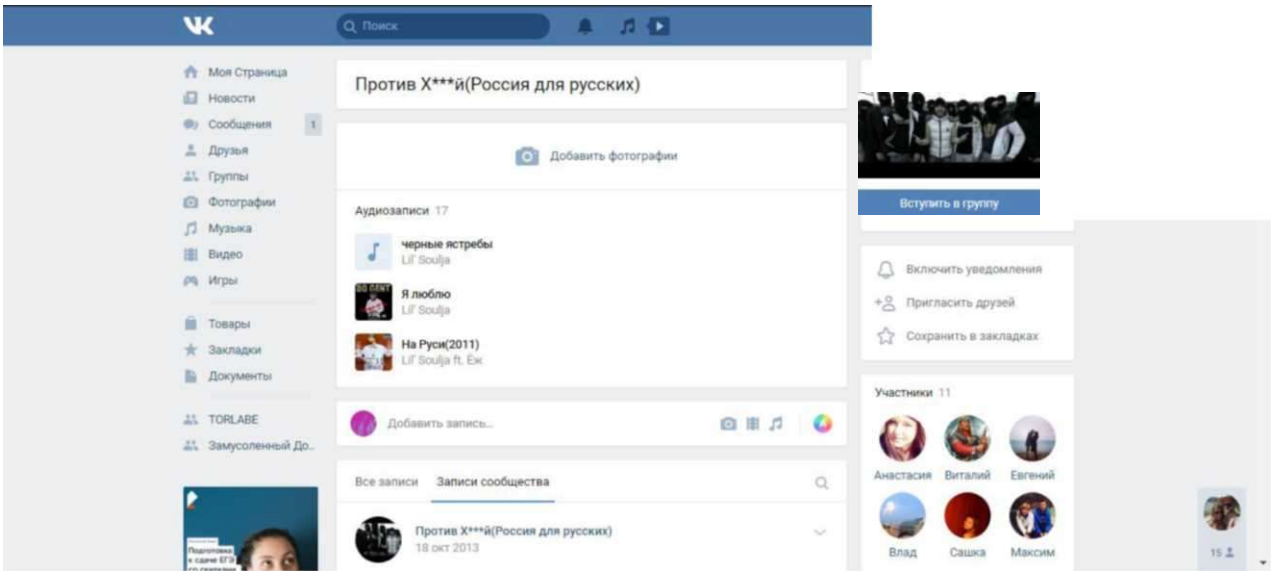
Как осуществлять поиск противоправного контента.

1. Находим в поиске группу с, предположительно, экстремистским контентом **(обязательно убираем в параметрах галочку «безопасный поиск», в этом случае нам высветятся ВСЕ группы).**

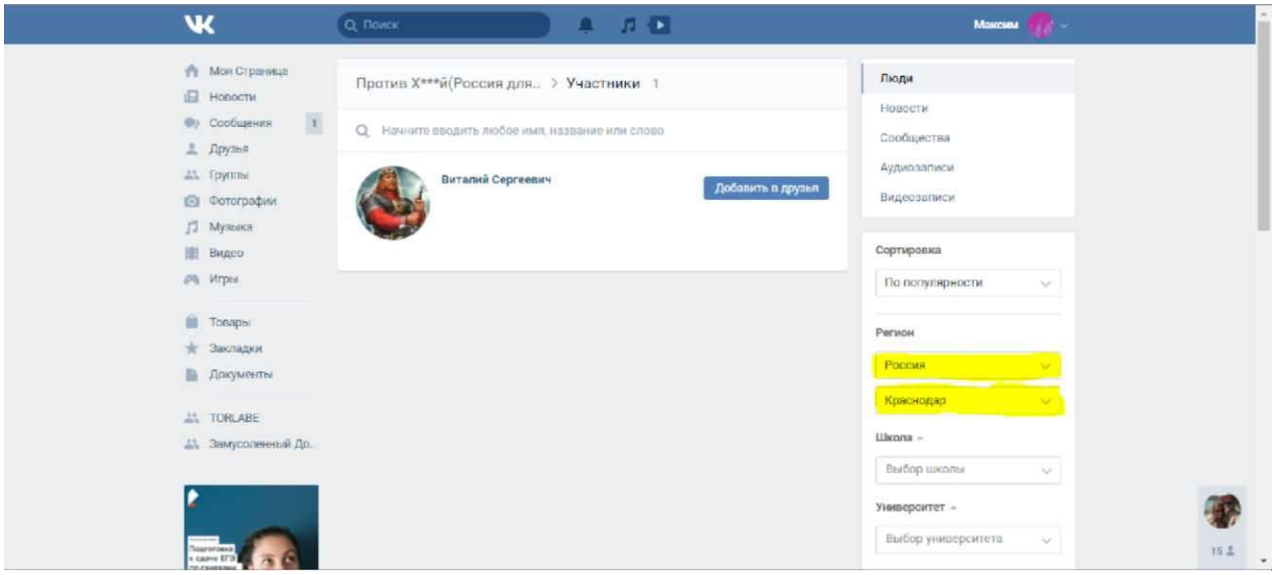
Заходим в группу. Просматриваем контент. Если контент является потенциально противоправным, то нажимаем на участников.



Далее выставляем нужные фильтры, а именно: возраст участника и город.



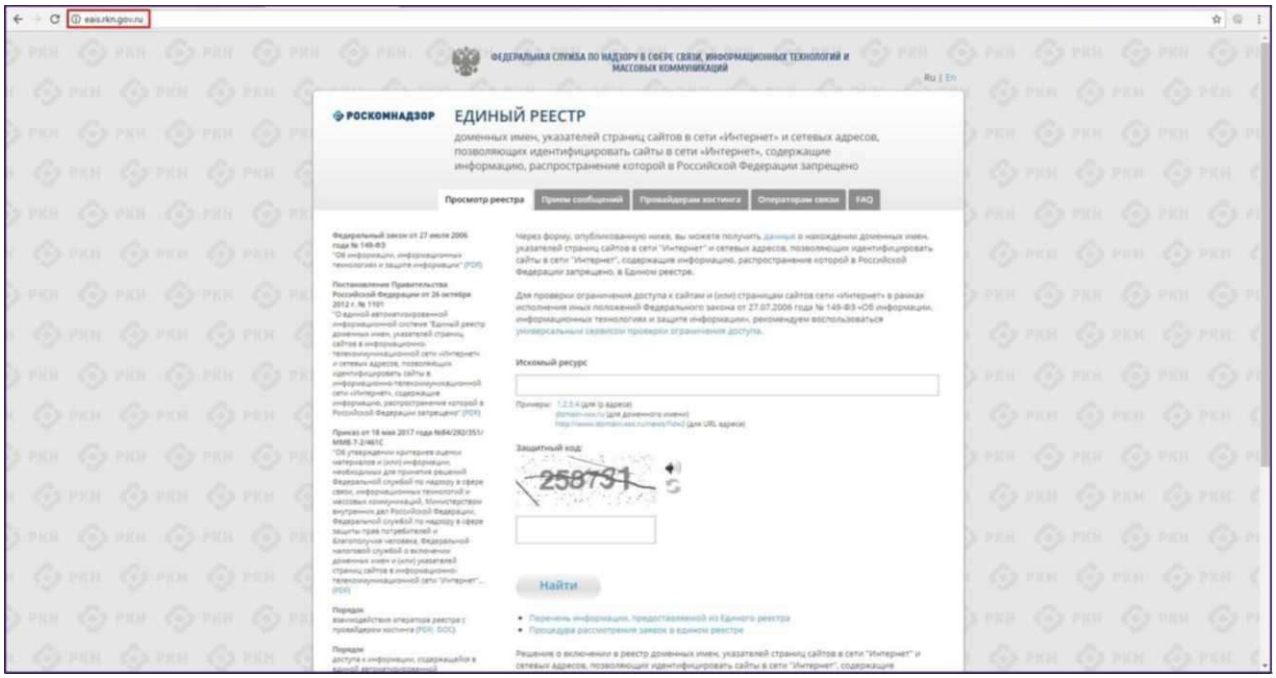
Помните, что в разделе «регион» высвечивается не весь край, а именно указанный город. Нужно мониторить каждый город своего региона.



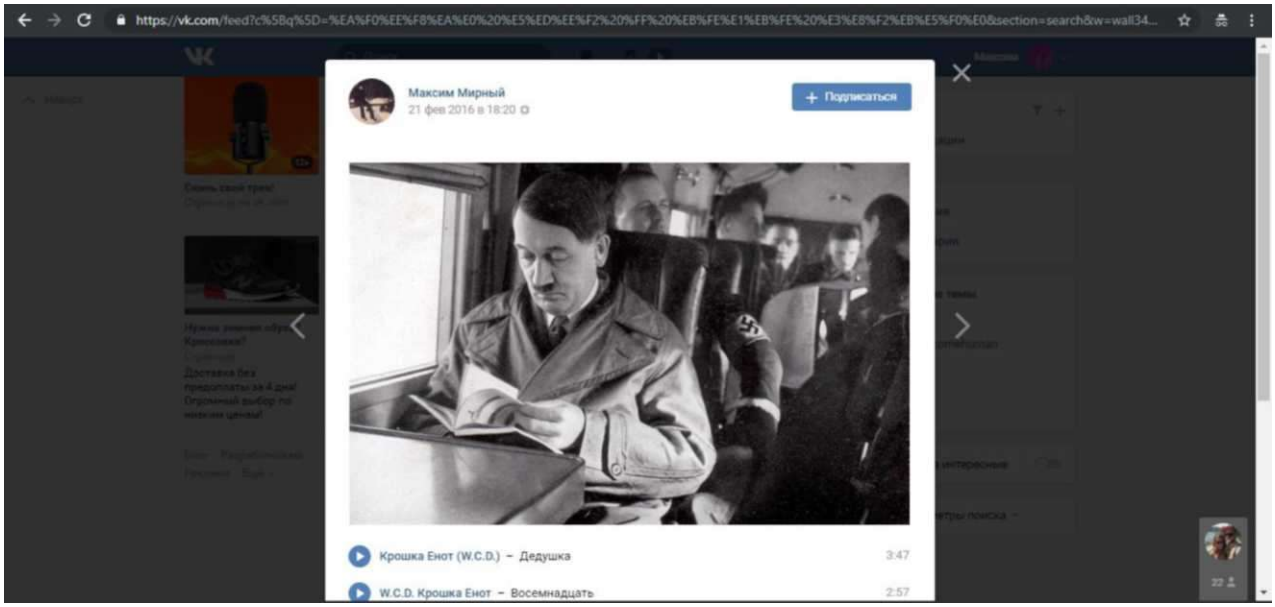
В результате мы получаем список участников, которые входят в группу риска.

Как правильно разместить выявленный материал на сайте Роскомнадзора

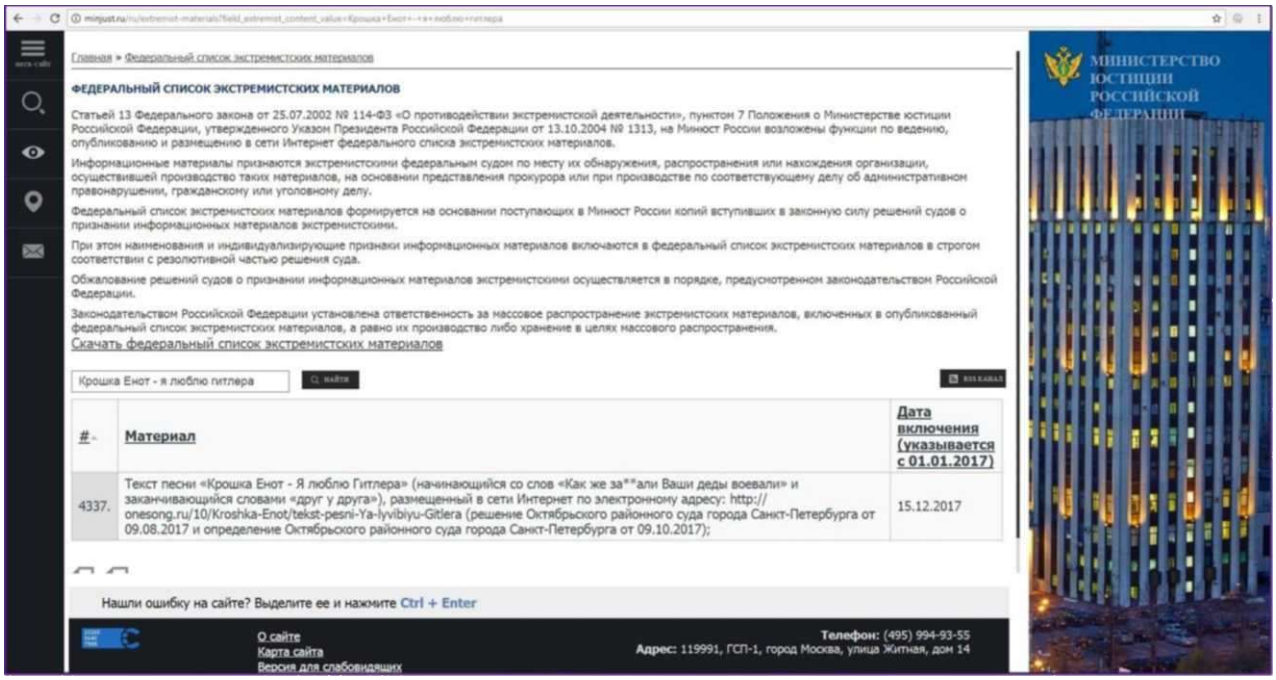
1. Открываем сайт https://eais.rkn.gov.ru.



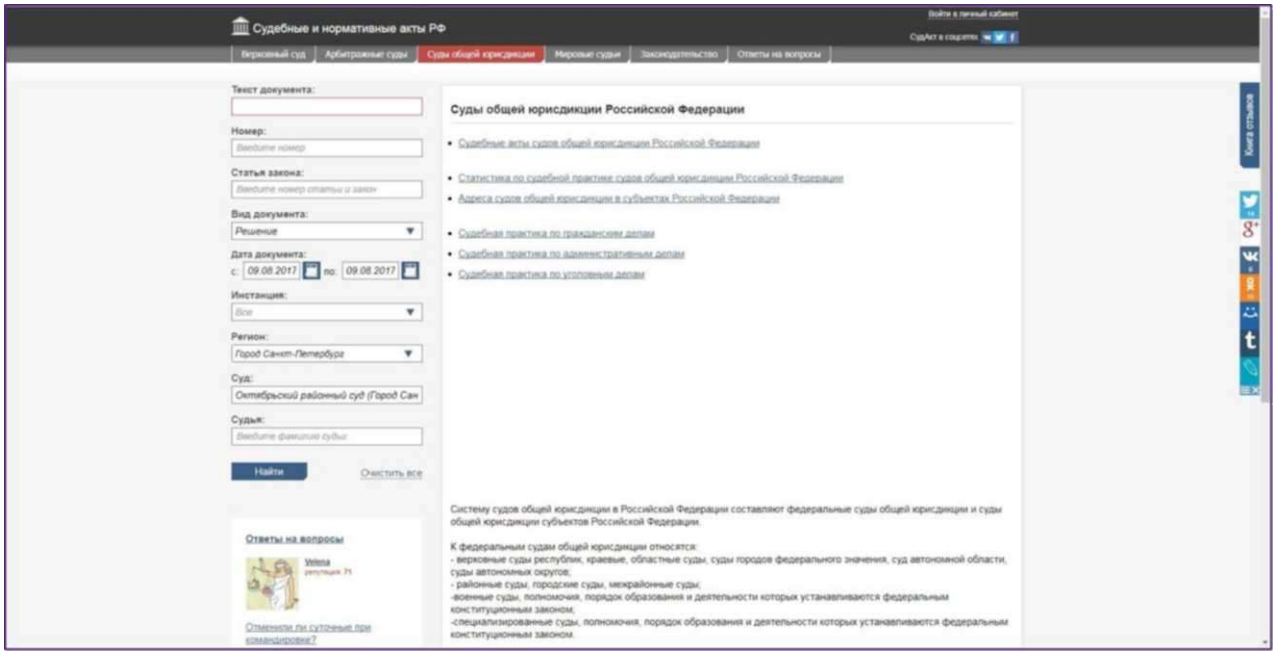
2. Делаем скриншот выявленного материала **(ОЧЕНЬ ВАЖНО СДЕЛАТЬ СКРИНШОТ ТАК, ЧТОБЫ БЫЛО ВИДНО ССЫЛКУ НА ВЫЯВЛЕННЫЙ МАТЕРИАЛ).**



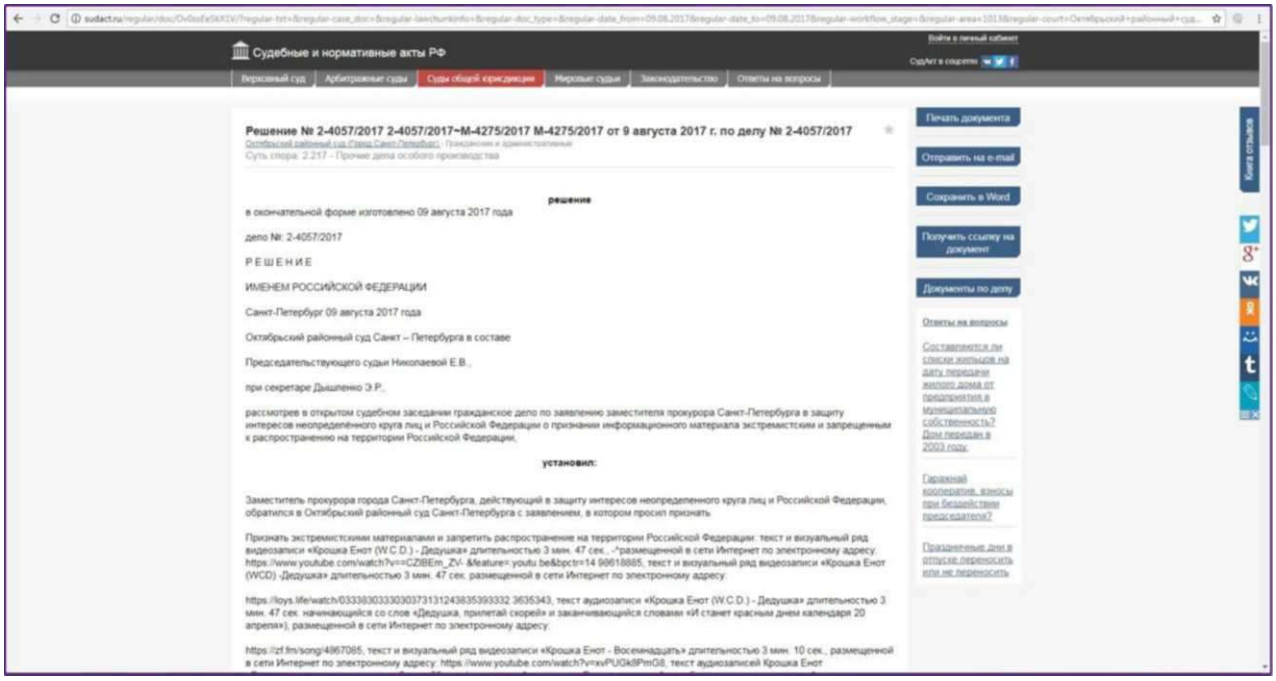
3. Находим описание выявленного материала в ФСЭМ (Федеральном списке экстремистских материалов).



4. Открываем базу судебных решений sudact.ru или сайт суда, который рассматривал дело о внесении материала в ФСЭМ.



5. Находим решение по выявленному материалу.



6. Используя полученные данные, заполняем форму на сайте Роскомнадзора.

Подать сообщение о ресурсе, содержащем запрещенную информацию

** - поля, обязательные для заполнения*

Тип информации *	судебное решение, экстремистские материг
Указатель страницы сайта в сети "Интернет" * **с обязательным указанием протокола** **допустимо указание до 50 URL адресов, один** **адрес на строку**	https://vk.com/id40381715
Источник информации	веб-сайт

Скриншот (pdf. jpeg. png не более 1 Мб)	Выберите файл ScreenshoMOjpg
Судебное решение	
наименование суда *	Октябрьский районный суд г. Санкт-Петербург
Номер дела *	№2-4057/2017
Дата решения *	09.08.2017
Ссылка на решение суда, размещенное на официальном информационном ресурсе *	http://sudact.ru/regu ar/doc/OvOssEeSkXW/Tregi
Файл решения * (pdf. riff, jpeg png; не более 10Мб)	Выберите файл Решение 2... 2017.rtf

5. 7. Делаем скриншот заполненной формы, формируем отчет и направляем в адрес руководителям и отделению безопасности ОБПОУ «КБМК».

Что делать с выявленными случаями кибербуллинга

Если при осуществлении мониторинга вы выявили факт кибербуллинга, необходимо совершить следующие действия:

1. Сделать скриншот;
2. Сохранить ссылку на страницу человека, который осуществил кибербуллинг;
3. Сохранить ссылку на пост, где вы обнаружили факт кибербуллинга;
4. Подготовить отчет и направить его руководителю местного отделения;

Что делать с выявленными случаями подстрекательства к совершению противоправных действий (совершение террористического акта, призывы к совершению преступлений и т.д.)

Если при осуществлении мониторинга вы выявили факт подстрекательства к совершению противоправных действий, необходимо совершить следующие действия:

1. Сделать скриншот;
2. Сохранить ссылку на страницу человека, который совершил подстрекательство;
3. Сохранить ссылку на пост, где вы обнаружили факт подстрекательства;
4. Направить информацию руководителям и отделению безопасности ОБПОУ «КБМК», а также незамедлительно сообщить ему о выявленном факте;

8 признаков вербовщика террористической организации

Что делать с выявленными случаями вербовки

Если при осуществлении мониторинга вы выявили факт вербовки, необходимо совершить следующие действия:

1. Сделать скриншот;
2. Сохранить ссылку на страницу человека, который осуществляет вербовку;

3. Сохранить ссылку на пост, где вы обнаружили предположительный случай вербовки;

4. Направить информацию руководителю местного отделения и незамедлительно сообщить ему о выявленном факте;

5.

Основная терминология по профилактике экстремизма и идеологии терроризма

Согласно статье 1 Федерального закона «О противодействии экстремистской деятельности» № 114-ФЗ от 25 июля 2002 года: 1) **экстремистская деятельность (экстремизм):**

- насильственное изменение основ конституционного строя и нарушение целостности Российской Федерации;
- публичное оправдание терроризма и иная террористическая деятельность;
- возбуждение социальной, расовой, национальной или религиозной розни;
- пропаганда исключительности, превосходства либо неполноценности человека по признаку его социальной, расовой, национальной, религиозной или языковой принадлежности, или отношения к религии;
- нарушение прав, свобод и законных интересов человека и гражданина в зависимости от его социальной, расовой, национальной, религиозной или языковой принадлежности, или отношения к религии;
- воспрепятствование осуществлению гражданами их избирательных прав и права на участие в референдуме или нарушение тайны голосования, соединенные с насилием либо угрозой его применения;
- воспрепятствование законной деятельности государственных органов, органов местного самоуправления, избирательных комиссий, общественных и религиозных объединений или иных организаций, соединенное с насилием либо угрозой его применения;
- совершение преступлений по мотивам, указанным в пункте "е" части первой статьи 63 Уголовного кодекса Российской Федерации;
- пропаганда и публичное демонстрирование нацистской атрибутики или символики либо атрибутики или символики, сходных с нацистской атрибутикой или символикой до степени смешения, либо публичное демонстрирование атрибутики или символики экстремистских организаций;
- публичные призывы к осуществлению указанных деяний либо массовое распространение заведомо экстремистских материалов, а равно их изготовление или хранение в целях массового распространения;
- публичное заведомо ложное обвинение лица, замещающего государственную должность Российской Федерации или государственную должность субъекта Российской Федерации, в совершении им в период исполнения своих должностных обязанностей деяний, указанных в настоящей статье и являющихся преступлением;

- организация и подготовка указанных деяний, а также подстрекательство к их осуществлению;
- финансирование указанных деяний либо иное содействие в их организации, подготовке и осуществлении, в том числе путем предоставления учебной, полиграфической и материально-технической базы, телефонной и иных видов связи или оказания информационных услуг.

2) **экстремистская организация** - общественное или религиозное объединение либо иная организация, в отношении которых по основаниям, предусмотренным настоящим Федеральным законом, судом принято вступившее в законную силу решение о ликвидации или запрете деятельности в связи с осуществлением экстремистской деятельности;

3) **экстремистские материалы** - предназначенные для обнародования документы либо информация на иных носителях, призывающие к осуществлению экстремистской деятельности либо обосновывающие или оправдывающие необходимость осуществления такой деятельности, в том числе труды руководителей национал-социалистской рабочей партии Германии, фашистской партии Италии, публикации, обосновывающие или оправдывающие национальное и (или) расовое превосходство либо оправдывающие практику совершения военных или иных преступлений, направленных на полное или частичное уничтожение какой-либо этнической, социальной, расовой, национальной или религиозной группы;

4) **символика экстремистской организации** - символика, описание которой содержится в учредительных документах организации, в отношении которой по основаниям, предусмотренным настоящим Федеральным законом, судом принято вступившее в законную силу решение о ликвидации или запрете деятельности в связи с осуществлением экстремистской деятельности.

В статье 3 Федерального закона «О противодействии терроризму» № 35-ФЗ от 6 марта 2006 года используются следующие основные понятия:

1) **терроризм** - идеология насилия и практика воздействия на принятие решения органами государственной власти, органами местного самоуправления или международными организациями, связанные с устрашением населения и (или) иными формами противоправных насильственных действий;

2) **террористическая деятельность** - деятельность, включающая в себя:

а) организацию, планирование, подготовку, финансирование и реализацию террористического акта;

б) подстрекательство к террористическому акту;

в) организацию незаконного вооруженного формирования, преступного сообщества (преступной организации), организованной группы для реализации террористического акта, а равно участие в такой структуре;

г) вербовку, вооружение, обучение и использование террористов;

д) информационное или иное пособничество в планировании, подготовке или реализации террористического акта;

е) пропаганду идей терроризма, распространение материалов или информации, призывающих к осуществлению террористической деятельности либо обосновывающих или оправдывающих необходимость осуществления такой деятельности;

3) **террористический акт** - совершение взрыва, поджога или иных действий, устрашающих население и создающих опасность гибели человека, причинения значительного имущественного ущерба либо наступления иных тяжких последствий, в целях дестабилизации деятельности органов власти или международных организаций либо воздействия на принятие ими решений, а также угроза совершения указанных действий в тех же целях;

4) **противодействие терроризму** - деятельность органов государственной власти и органов местного самоуправления, а также физических и юридических лиц по:

а) предупреждению терроризма, в том числе по выявлению и последующему устранению причин и условий, способствующих совершению террористических актов (профилактика терроризма);

б) выявлению, предупреждению, пресечению, раскрытию и расследованию террористического акта (борьба с терроризмом);

в) минимизации и (или) ликвидации последствий проявлений терроризма;

5) **контртеррористическая операция** - комплекс специальных, оперативно-боевых, войсковых и иных мероприятий с применением боевой техники, оружия и специальных средств по пресечению террористического акта, обезвреживанию террористов, обеспечению безопасности физических лиц, организаций и учреждений, а также по минимизации последствий террористического акта;

6) **антитеррористическая защищенность объекта (территории)** - состояние защищенности здания, строения, сооружения, иного объекта, места массового пребывания людей, препятствующее совершению террористического акта. При этом под местом массового пребывания людей понимается территория общего пользования поселения или городского округа, либо специально отведенная территория за их пределами, либо место общего пользования в здании, строении, сооружении, на ином объекте, на которых при определенных условиях может одновременно находиться более пятидесяти человек.

Основная терминология, связанная с кибербуллингом

Кибербуллинг (электронная травля, жестокость онлайн) - это вид травли, преднамеренные агрессивные действия систематически на протяжении длительного периода, осуществляемые группой или индивидом с использованием электронных форм взаимодействий, направленных против жертвы, которая не может себя защитить. Это может происходить через смс-сообщения, социальные сети, создание компрометирующих веб-страниц или размещение унижающего, оскорбляющего видеоконтента и так далее.

Троллинг (cyber trolls) - это ситуации, когда именно агрессоры публикуют негативную, тревожащую информацию на веб-сайтах, страницах социальных сетей, даже на мемориальных страницах, посвященных умершим людям.

Хейтинг (hate) - это негативные комментарии и сообщения, иррациональная критика в адрес конкретного человека или явления, часто без обоснования своей позиции.

Флэйминг (flaming) - это вспышка оскорблений, публичный эмоциональный обмен репликами, часто разгорается в чатах и комментариях в социальных сетях. Так как это происходит публично, большое количество людей могут спонтанно подключаться к оскорблениям одной из сторон конфликта. Часто бывает, что одна из сторон ставит целью вовлечение большого количества случайных свидетелей в противостояние.

Кибersталкинг (cyberstalking; to stalk - преследовать, выслеживать) -использование электронных коммуникаций для преследования жертвы через повторяющиеся угрожающие, вызывающие тревогу и раздражение сообщения с намерением напугать жертву угрозой противозаконных действий или повреждений, которые могут быть осуществлены с получателем сообщений или членами его семьи.

Грифинг (griefers) - это процесс, в котором игроки целенаправленно преследуют других игроков в многопользовательских онлайн-играх. Их цель не победить в игре, а лишить удовольствия от игры других. Их легко можно узнать: они активно используют брань, блокируют отдельные области игры и открыто мошенничают в игре, также они могут использовать более опасные методы воздействия на играющего (например, разместить специально созданную мигающую панель с движущимися объектами, провоцирующую у игроков эпилептический приступ).

Секстинг (sexting) - это процесс рассылки или публикация фото- и видеоматериалов с обнаженными и полуобнаженными людьми. Чем старше дети, тем выше вероятность их вовлечения в секстинг. Иногда сообщения рассылают в рамках парных отношений, в других случаях преследуют при этом цели травли и нанесения вреда, например, выкладывая в «Интернет» обнаженные фото бывшей партнерши в качестве мести за болезненный разрыв отношений. Получение такого рода сообщений может вызвать сильную тревогу у молодого человека.